Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№08 (241)/2013

АУТСОРСИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

WWW.JETINFO.RU

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:
Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Шедова Е.Л.

Шкляева А.Л.
ashklyaeva@jet.msk.su

Верстка:
Полевщикова Д.М.

Корректура:
Макеева Е.И.

Над номером работали:
Акимов Е.О.
Бейбутов Э.Р.
Дрюков В.В.
Костина А.Б.
Лаврухин А.Ю.
Михеев Д.С.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
http://www.jetinfo.ru

ЕВГЕНИЙ АКИМОВ,
заместитель директора Центра информационной безопасности компании «Инфосистемы Джет»

Сделать большее за те же деньги. Сделать невозможное за разумные деньги. Сделать, не вложив ни копейки. Что это — утопия? Мечты идиота?

Всё это сулит использование аутсорсинга. ИБ-аутсорсинга. И хочется, и боязно. Дать доступ в святая святых в погоне за экономией? А будет ли она? Кто вообще обещает, что аутсорсинг — это дёшево?

Этот номер целиком и полностью посвящен теме ИБ-аутсорсинга. Время его выхода — момент перехода от обсуждения темы к появлению рынка спроса и предложения, время заключения полноценных аутсорсинговых контрактов. В номере мы обсуждаем и самые общие вопросы — что в принципе можно отдать (и принять!) на аутсорсинг, и вполне конкретные, например, использование облачных SOC, а также затрагиваем темы завтрашнего дня — противодействие APT (Advanced Persistent Threat).

P.S. Нам важно ваше мнение. Уделите нам минуту и оцените номер на сайте www.jetinfo.ru.

СОДЕРЖАНИЕ

Подробности защиты Программы МАЛИНА от DDoSеров

малина™

Программа МАЛИНА (управляющая компания «Лоялти Партнерс Восток») и компания «Инфосистемы Джет» рассказали о подробностях успешного отражения одной из самых мощных в России DDoS-атак, целью которой стали ресурсы Программы. Атака состояла из нескольких этапов, была ориентирована на web-серверы и ряд инфраструктурных сервисов Программы. Ее продолжительность составила более двух суток, а объем нелегитимного трафика, направленного злоумышленниками на ресурсы Программы, превысил 40 Гбит в секунду.

Для эффективного отражения атаки и восстановления работы всех сервисов Программы в сжатые сроки была сформирована экспертная группа, в которую вошли специалисты Сервисного центра и Центра информационной безопасности компании «Инфосистемы Джет», обладающие необходимыми компетенциями. Был проанализирован характер трафика, сформированы и направлены провайдеру для последующей блокировки «черные списки» IP-адресов, с которых велась атака. Это позволило сбить первую волну DDoS. В дата-центре компании «Лоялти Партнерс Восток» был установлен межсетевой экран (Cisco ASA) и развернут программный комплекс мониторинга, проведена повторная диагностика сетевого трафика и установлено, что злоумышленники начали использовать подложные IP-адреса. Это потребовало оперативного подключения внешнего сервиса защиты от DDoS-атак – Kaspersky DDoS Prevention (KDP), который обеспечил максимальную фильтрацию поступающих запросов.

Принятые меры в совокупности позволили оперативно отразить DDoS-атаку и полностью восстановить работоспособность всех сервисов и сайтов компании.

«Данный случай можно считать своего рода показательным, наглядно продемонстрировавшим прямую зависимость между продуктивным решением бизнес-задач и эффективной организацией ИБ, – комментирует **ЕВГЕНИЙ АКИМОВ**, заместитель директора Центра информационной безопасности компании "Инфосистемы Джет". *– По итогам выполненных работ мы предложили компании "Лоялти Партнерс Восток" скорректировать комплексный план дальнейшего развития информационной безопасности с учетом таких задач, как защита публичных и внутренних сервисов, организация эффективного мониторинга и управления информационной безопасностью в режиме 24/7 на базе Jet Security Operation Center».*

«Компания "Инфосистемы Джет" осуществляет комплексный аутсорсинг ИТ-инфраструктуры Программы МАЛИНА с 2006 года. В момент совершения атаки средства мониторинга работоспособности оборудования начали сигнализировать о чрезмерной нагрузке, эксперты Сервисного центра компании приняли оперативные меры и привлекли к дальнейшей работе специалистов Центра информационной безопасности. Вектор и способы атаки постоянно менялись, что требовало оперативных мер защиты, при этом особенно хочется отметить высокий уровень профессионализма наших партнеров в отражении DDoS-атаки, оперативность, нацеленность на результат и по-настоящему командную работу – это позволило совместными усилиями успешно отразить атаку», – резюмирует Операционный директор компании «Лоялти Партнерс Восток» **ДЕНИС КРУЧИНИН**. JI

Сертификация от Cisco по решениям ВКС

Компания «Инфосистемы Джет» получила технологическую специализацию Cisco ATP TelePresence Video Express, которая подтверждает соответствие требованиям вендора к своим партнерам в сфере внедрения и технической поддержки ВКС-решений Cisco. Продукты, представленные в линейке Cisco TelePresence, особенно актуальны при организации многоточечных конференций для проведения переговоров, удаленных презентаций, демонстраций, обучения и т.п.

«Наша практика показывает, что за последний год на отечественном рынке существенно выросла популярность технологий видеосвязи и телеприсутствия. Мы достаточно часто сталкиваемся с запросами на реализацию систем ВКС, — говорит **АЛЕКСЕЙ ДОГАЕВ**, директор Центра сетевых решений компании "Инфосистемы Джет". *— Линейка решений Cisco TelePresence хорошо внедряется в инфраструктуру компаний, построенную на оборудовании Cisco. При этом особенно интересные решения получаются при*

интеграции с системами унифицированных коммуникаций — Cisco Unified Communications Manager».

В демо-лаборатории компании развернут стенд, на котором в условиях, максимально приближенных к «боевым», можно ознакомиться с решениями ВКС для оснащения переговорных комнат и рабочих мест системами в формате Full HD с возможностью организации конференций в многоточечном режиме. На данный момент реализовано несколько комплексных проектов в сфере ВКС для компаний различных отраслей.

«В последние годы решения по обеспечению телеприсутствия (TelePresence) приобретают все большую популярность и находятся в числе наиболее перспективных технологий, которые будут задавать тон на мировом рынке телекоммуникаций. Комплексное решение Cisco TelePresence обеспечивает живое общение лицом к лицу, позволяя осуществлять как никогда эффективное взаимодействие, — комментирует **ВЛАДИМИР ЯРОСЛАВСКИЙ**, менеджер по продвижению новых технологий Cisco. — *Профессиональная подготовка экспертов компании "Инфосистемы Джет", накопленная экспертиза и высокий уровень удовлетворенности заказчиков по итогам проектов, выполненных с использованием технологий Cisco, позволили нам сертифицировать партнера в сфере технологий ВКС и в очередной раз подтвердить его наивысший партнерский статус».*

Компания «Инфосистемы Джет» является «золотым» партнером Cisco с 2008 года и на сегодняшний день обладает 8 специализациями Cisco уровня Advanced. JI

Новая версия ОС от NetApp

NetApp™

Компания NetApp выпустила новую версию операционной системы Clustered Data ONTAP. Новое ПО позволит различным организациям, в том числе поставщикам облачных услуг, обеспечивать максимальную готовность приложений и быстро предоставлять необходимые услуги без увеличения затрат. Clustered Data ONTAP 8.2 устраняет все ограничения производительности, готовности и эффективности, характерные для традиционных СХД, позволяя ИТ-отделам адаптировать инфраструктуру хранения данных к меняющимся потребностям бизнеса и приложений без прерывания рабочих процессов.

В решении собраны функции:

- непрерывность операций: постоянный доступ к данным во время запланированных простоев и динамическое распределение нагрузки без переноса данных, влияющего на производительность;
- масштабируемость: до 69 ПБ памяти и 24 контроллерных узлов, 49 000 томов LUN, 12 000 томов NAS с поддержкой свыше 100 000 клиентов.
- операционная эффективность СХД: унифицированная архитектура с поддержкой многопользовательской среды, которая соответствует практически всем требованиям SMB-компаний. JI

RSA борется со злонамеренными действиями в интернете

Компания RSA выпустила новую версию решения для обнаружения веб-угроз RSA Silver Tail. Версия 4.0 позволит организациям лучше визуализировать активность на веб-сайтах, чтобы отделять нормальное поведение от потенциально злонамеренного. Получив такую возможность, отделы ИБ и специалисты по борьбе с интернет-мошенничеством смогут в реальном времени отслеживать и нейтрализовывать угрозы, связанные с веб-сеансами и мобильными приложениями.

RSA Silver Tail предоставляет средства, при помощи которых можно идентифицировать большее количество угроз за меньшее время и с большей эффективностью. Кроме того, оно дополнено функциями управления инцидентами за один клик и интеллектуальным пользовательским интерфейсом, который позволяет лучше визуализировать активность на веб-сайте, используя данные миллионов одновременных веб-сеансов. Благодаря платформе Streaming Analytics и функции последовательной оценки угроз технология RSA Silver Tail 4.0 использует возможности Больших Данных для идентификации угроз, злонамеренного трафика и значимых отклонений поведения, которые не могут быть выявлены только путем анализа журналов веб-сеансов. В результате компании могут добиться снижения прямых и непрямых расходов, связанных с мошенничеством, нарушениями безопасности или злонамеренными действиями на веб-сайтах, такими как захват аккаунтов, угадывание паролей, DDoS-атаки, скрейпинг сайтов и злоупотребления бизнес-логикой (например, эксплуатация функции корзины или интернет-скидок).

Преобразуя последовательности кликов в аналитические данные веб-сеансов, решение предоставляет компаниям прозрачность для выявления принципиальных различий между обычными действиями пользователей и злонамеренными действиями, которые выполняются на веб-сайтах интернет-магазинов, веб-порталах электронного правительства и интернет-банкинга. JI

ДИНАМИЧЕСКАЯ ИТ-ИНФРАСТРУКТУРА ДЛЯ ФГ ЛАЙФ

Финансовая Группа Лайф, в состав которой входят Пробизнесбанк и 6 региональных банков, развивается стремительными темпами. Постоянно расширяется портфель услуг, увеличивается количество отделений и клиентов, возрастает нагрузка на системы. Для обеспечения быстрых изменений в бизнесе компании необходимо было трансформировать подход к формированию ИТ-платформы Группы. В 2010 году в партнерстве с компанией «Инфосистемы Джет» был выбран курс на создание динамической ИТ-инфраструктуры.

Для реализации данной концепции были выбраны унифицированная аппаратная платформа и механизмы защиты данных основных банковских систем. Все базы данных и приложения были вынесены в единое внешнее хранилище. 26 сетей хранения SAN объединены в общую иерархическую структуру. Все серверные приложения и серверы баз данных перенесены в виртуальную среду VMware vSphere и IBM SVC.

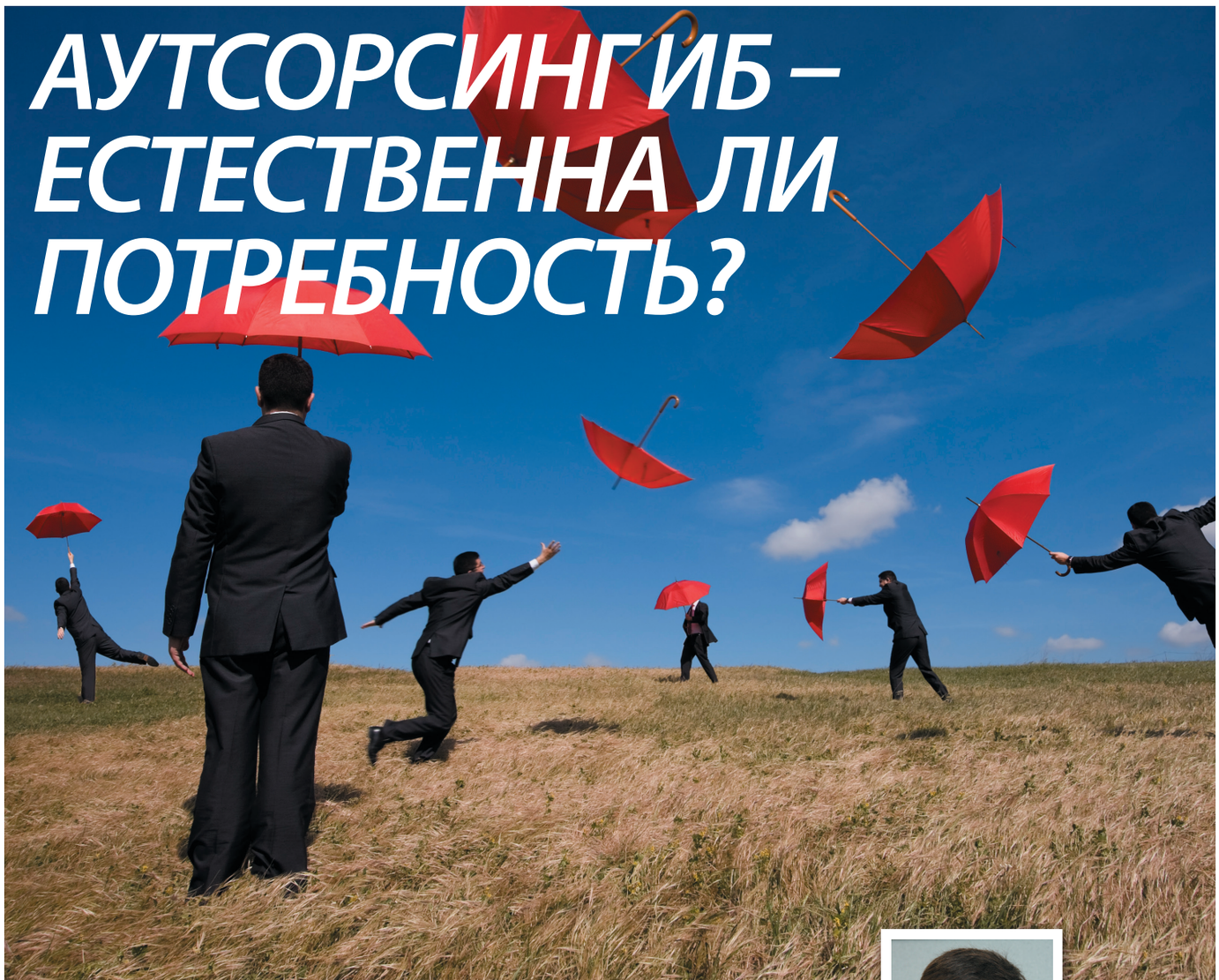
Унифицированы и консолидированы компоненты ИТ-инфраструктуры бизнес-критичных приложений: системы процессинга OpenWay и трех АБС (RSBank, FrontLife, Interbank). Внедрены механизмы автоматической миграции вычислительных задач между серверами и системами хранения данных без остановки бизнес-процессов (на случай нештатных ситуаций или проведения сервисных работ).

Консолидация компонентов ИТ-инфраструктуры значительно улучшила использование существующих вычислительных ресурсов. Благодаря распределению нагрузки на дисковые массивы и серверы удалось высвободить значительные ресурсы для увеличения производительности существующих приложений и внедрения новых систем. Существенно повысились отказоустойчивость и производительность информационных систем: при необходимости они могут пользоваться аппаратными ресурсами друг друга, не прерывая своей работы. Теперь для создания ИТ-инфраструктуры для новых банковских приложений требуется не более 1 недели, тогда как раньше на это уходило до 4 месяцев.

«Благодаря динамической ИТ-инфраструктуре банки Группы теперь могут быстрее выводить новые продукты на рынок, быстро трансформировать ИТ-инфраструктуру при поглощении новых бизнесов и т.п., — сообщил **ДЕНИС ГАРЕВСКИЙ**, начальник управления дистанционного банковского обслуживания Пробизнесбанка. — *Кроме того, повысилось качество технического обслуживания клиентов: если в какой-то из систем произойдет сбой на уровне серверов приложений или обнаружится нехватка дискового пространства, конечные пользователи этого даже не заметят».*

«Группа Лайф получила гибкую ИТ-инфраструктуру, которая позволяет своевременно отвечать на меняющиеся запросы бизнеса, — отметил **АНДРЕЙ ШАПОШНИКОВ**, заместитель директора Центра проектирования вычислительных комплексов компании "Инфосистемы Джет". — *Задачи следующего совместного проекта, над которым мы работаем, — построение системы учета ресурсов и переход к поставке информационных услуг в виде сервисов».* JI

АУТСОРСИНГ ИБ – ЕСТЕСТВЕННА ЛИ ПОТРЕБНОСТЬ?



АЛЕКСЕЙ ЛАВРУХИН,
директор по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет»

Тема аутсорсинга ИБ в последнее время активно набирает популярность в профессиональном сообществе специалистов по защите информации, а также становится все более заметной на рынке в целом. Ей посвящаются секции и круглые столы крупнейших профильных конференций, ответственные за обеспечение ИБ в крупных компаниях обсуждают между собой применимость такого подхода на практике, кто-то делится уже приобретенным опытом реализации подобных проектов.

Прежде чем переходить к системному изложению нашего подхода к решению этой задачи в крупных компаниях, хотелось бы поделиться нашим взглядом

на причины возникновения темы как таковой, а также ответить на вопрос: «Является ли спрос на услуги аутсорсинга ИБ естественной потребностью, вызванной ростом уровня зрелости процессов обеспечения ИБ в российских компаниях, либо это искусственно создаваемый интерес к модной нынче теме?». Для этого приведем наиболее часто встречаемые поводы для начала разговора об ИБ-аутсорсинге со стороны потенциальных и реальных заказчиков данной услуги.

В нашей практике нередки случаи, когда крупные компании, особенно финансового и страхового сектора, хотят ограничить «зоны влияния» собственного ИБ-персонала. Задачей обеспечения безопасности информации они занимаются уже довольно давно, поэтому зачастую сложность систем защиты, так же как и количество уникальных компетенций обслуживающего их персонала, достигает высокого уровня. В какой-то момент руководство понимает, что ключевые знания о том, как должны функционировать механизмы обеспечения ИБ, как правильно настраивать средства защиты и управлять ими, содержатся исключительно в головах ответственных за ИБ специалистов. Они не закреплены в полной мере в документальном виде. Поэтому увольнение подобных сотрудников либо переход всей команды в другую компанию приведет к фактической остановке процессов обеспечения информационной безопасности. Топ-менеджмент окажется в затруднительном положении, оставшись с глазу на глаз со всеми ИТ-угрозами и рисками без должной поддержки. Зачастую ситуация усугубляется фактом перехода сотрудников к прямому конкуренту, который вместе с квалифицированным персоналом получает информацию об архитектуре и уязвимостях систем защиты соседа по рынку.

Другой пример — компании, активно и успешно отдающие на аутсорсинг обслуживание ИТ-систем как непрофильное для себя направление деятельности (например, ритейлеры). Зачастую в связи с кажущейся на первый взгляд независимостью функционирования основных бизнес-процессов компании от работы ИТ руководство не уделяет достаточного внимания вопросам обеспечения безопасности данных, обрабатываемых информационными системами. Однако рыночная конкуренция требует все более быстрого принятия решений, поэтому степень проникновения ИТ в таких компаниях неизбежно растет. При этом профессиональный ИТ-аутсорсер, обслуживающий системы организации, может гарантировать уровень сервиса в части работоспособности, доступности и восстановления ИТ-ландшафта, но никак не защищенность обрабатываемых данных.

Такие компании приходят к осознанию необходимости решения вопросов ИБ по-разному, но обычно вследствие возникновения каких-либо серьезных неприятностей, например утечки незащищенных конфиденциальных данных, или проверки регулятором режима обработки персональных данных на соответствие законодательству. Сразу после этого заказчик обращается к своему ИТ-аутсорсеру с требованием взять на себя в том числе решение задач обеспечения ИБ. Однако тот в подавляющем большинстве случаев разводит руками и ссылается на отсутствие необходимых для такого рода услуг компетенций и инфраструктуры. Тогда заказчику приходится искать подобные предложения на рынке...

По опыту мы знаем, что аутсорсинг ИБ также интересен компаниям, на первый взгляд совсем не

похожим на потенциального заказчика такого рода услуг. В них служба ИБ имеет значительный штат специалистов, регулярно выделяются бюджеты на покупку и развитие систем информационной безопасности, процессы управления ИБ правильно выстроены, задокументированы и постоянно модернизируются согласно стратегии планомерного развития на 3–5 лет. Однако XXI век не оставляет шанса на успех в случае отсутствия постоянных преобразований, зачастую носящих не эволюционный, а революционный характер. Новые направления деятельности, слияния и поглощения, рыночная ситуация — все это приводит к необходимости изменения существующих и создания новых бизнес-процессов, что в свою очередь провоцирует значительный рост ИБ-рисков.

Поэтому в самый неожиданный момент перед службой ИБ возникает задача защиты абсолютно нового для нее сегмента ИТ-ландшафта. Например, построения системы защиты от мошенничества в связи с появлением нового направления деятельности или крупными финансовыми потерями в результате мошеннических действий. При этом сроки, отведенные руководством для запуска сервиса, не позволяют системно подойти к приобретению и накоплению знаний по тематике, планомерно выстроить процессы и аккуратно подобрать соответствующую задаче систему. Выходом в такой ситуации становится использование необходимого сервиса из облака оператора профессиональных аутсорсинговых услуг ИБ с фиксированной ежемесячной платой и отсутствием капитальных вложений. В итоге сервис может выступить в роли и временного спасательного круга, позволив провести полноценный старт этого направления в компании, и постоянного решения.

Необходимость использования сервисов ИБ по аутсорсинговой модели может возникнуть и без каких-либо значительных изменений в структуре деятельности компании. Примером может служить возникающая по мере эволюционного развития ИБ потребность во внедрении центра оперативного управления и реагирования на инциденты ИБ (Security Operation Center). И тогда ключевыми проблемами могут стать как стоимость капитальных вложений на лицензии SIEM-решений и затраты на их внедрение, так и необходимость быстрого расширения штата службы ИБ (при мониторинге 24*7*365 плюс 7–8 специалистов). Обосновать и согласовать такое кадровое изменение крайне трудно, а эффективно эксплуатировать систему существующими ресурсами, при этом беря на себя обязательства по высокой скорости выявления и расследования инцидентов, невозможно из-за существующей загрузки специалистов.

Приведенные нами примеры возникающих у заказчиков задач показывают, что аутсорсинг ИБ — это реальная потребность рынка. При этом предложений — ответов на спрос — на данный момент явно не достаточно. Мы хотим поделиться опытом и наработками в организации подобного рода сервисов для своих клиентов, о чем и рассказываем в следующих статьях. JI

ОТДАТЬ НЕЛЬЗЯ ОСТАВИТЬ

ВЛАДИМИР ДРЮКОВ,
руководитель направления аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет»

Тематика аутсорсинга ИБ является одной из самых неоднозначных на рынке услуг информационной безопасности. Одним из ключевых факторов существующих противоречий является отсутствие четких договоренностей и понимания, какие именно услуги стоит относить к аутсорсингу ИБ и что вообще вкладывать в этот термин. Специалисты сферы ИТ, как правило, оценивают роль подразделения ИБ очень узко и понимают под словами «аутсорсинг информационной безопасности» техническое сопровождение используемых в компании средств защиты, руководство крупных компаний со своей стороны под этим термином подразумевает гораздо более широкую задачу — обеспечение безопасности организации и бизнеса.

Целью нашей статьи является попытка классифицировать и систематизировать функции подразделения информационной безопасности, выделить основные подходы к их реализации и определить возможности передачи данных задач на аутсорсинг. Весь

цикл обеспечения ИБ крупной компании можно условно разделить на 3 уровня:

- **оперативный:** включает в себя задачи сотрудников подразделения ИБ по прямому обеспечению информационной безопасности;
- **тактический:** включает в себя задачи по контролю процесса обеспечения ИБ, ответственность за него лежит на руководителе подразделения ИБ;
- **стратегический:** является задачей куратора информационной безопасности от руководства, на нем происходит определение общих целей и программы развития ИБ в компании.

Указанное разделение и основные задачи вкратце приведены на рис. 1.

При этом обсуждение вопросов аутсорсинга стоит начать с оперативного уровня как наиболее понятного и простого. Эти вопросы можно разделить на 2 области задач: технологические, основой реализации которых являются используемые в компании средства ИБ, и методологические, которые отталкиваются от нормативных требований и внутренних регламентов ИБ. Давайте рассмотрим каждую из областей подробнее.

Рис. 1. Уровни обеспечения ИБ и соответствующие им задачи

ОПЕРАТИВНЫЙ УРОВЕНЬ – ЭКСПЛУАТАЦИЯ СРЕДСТВ ЗАЩИТЫ ИЛИ СЕРВИС БЕЗОПАСНОСТИ

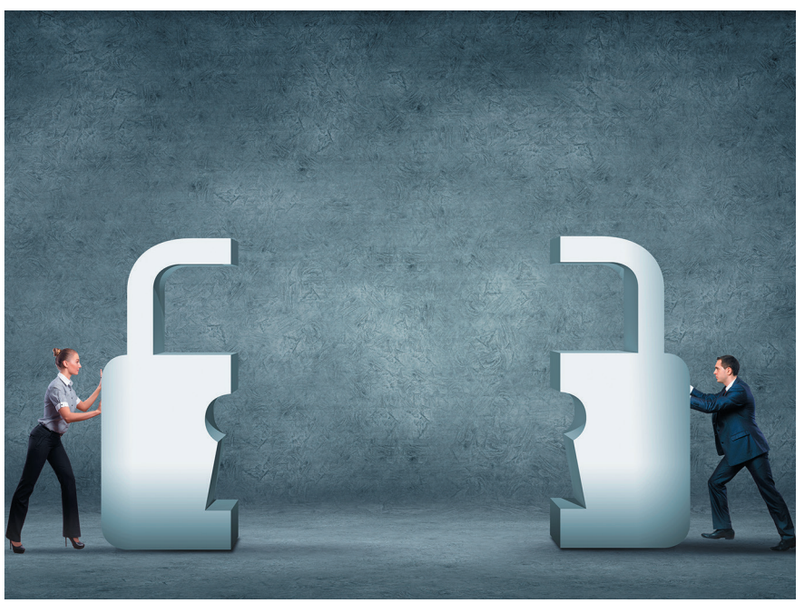
В рамках оперативных технологических функций отдела информационной безопасности можно выделить следующие основные задачи:

- обеспечение работоспособности систем ИБ компании. Несмотря на кажущуюся простоту, данная задача является одной из самых ресурсоемких в текущей жизни сотрудников ИБ. Количество систем информационной безопасности в компаниях с каждым годом растет и зачастую достигает двух десятков, сами системы одновременно с наращиванием своих функциональных возможностей становятся все более сложными в диагностике и ежедневном обслуживании.

Передача этой задачи внешнему подрядчику уже давно воспринимается компаниями достаточно естественно. Все чаще в тендерных конкурсах на построение системы можно видеть требования к последующему сервисному обслуживанию, включающие в себя ответственность интегратора за доступность и работоспособность системы в течение 3–5 лет и явно обозначающие необходимость проактивного мониторинга и контроля ее состояния;

- администрирование системы ИБ, которое часто включает в себя не только типовые активности по управлению конфигурацией (запуск/остановка процессов,

установка агентов, изменение системных параметров), но и содержательную с точки зрения информационной безопасности задачу по администрированию и созданию политик ИБ в рамках системы. Передача этих активностей внешнему подрядчику составляет большую сложность для компании, поскольку в случае online-системы интегратор осуществляет прямое управление доступом к тем или иным ресурсам, offline-системы — получает большой объем информации о



реализации корпоративных политик ИБ и общем уровне защищенности компании. Передача этой чувствительной и конфиденциальной задачи возможна только при высоком уровне доверия к подрядчику;

• реализация процессов обеспечения безопасности, которые практически неотделимы от соответствующей технологической платформы (контроль защищенности, управление инцидентами ИБ или контроль утечек конфиденциальной информации) и для которых задачи по обеспечению работоспособности и администрированию являются вспомогательными. Их построение и реализация собственными силами требуют как существенных изменений в кадровой структуре подразделения ИБ, например, выделения круглосуточной дежурной смены, так и наличия достаточно специфических компетенций у сотрудников, напрямую задействованных в их функционировании. Поэтому привлечение крупного интегратора, обладающего требуемыми компетенциями и ресурсами и способного обеспечить надлежащий уровень конфиденциальности получаемой информации, выглядит логичным ходом в развитии уровня безопасности компании.

Но эта задача, тем не менее, оставляет много вопросов как с точки зрения разграничения доступа к обрабатываемой информации, так и относительно эффективности применения внешних ресурсов для очень чувствительных к внутренним изменениям компании процессам. Например, при аутсорсинге управления инцидентами такие работы, как оценка влияния инцидента на бизнес-процессы, проверка применимости и согласование мер по противодействию ему, нетехническая сторона расследования, в том числе взаимодействие с внутренней службой безопасности и руководителями сотрудника, чаще всего практически невозможно отдать «на сторону». Сервис-провайдер, предоставляющий услугу, не в состоянии отслеживать и контролировать все внутренние структурные изменения в компании и обладать полной информацией о ее инфраструктуре и особенностях протекания бизнес-процессов, конечно, если он не оказывает услуг также и по их аутсорсингу. В связи с этим существует вероятность того, что противодействие инциденту информационной безопасности средней критичности негативно скажется на функционировании основных бизнес-процессов, что, безусловно, недопустимо. Поэтому вопрос о возможности передачи этих процессов на аутсорсинг требует детального исследования в каждом конкретном случае с учетом технической и организационной специфики их реализации.

ОПЕРАТИВНЫЙ УРОВЕНЬ – БЕЗОПАСНОСТЬ КАК СЕРВИС

В настоящее время часто можно наблюдать ситуацию, когда компании имеют острую необходимость в повышении собственного уровня безопасности за счет внедрения новых технологических платформ и построения сопутствующих им процессов, но не обладают возможностью совершать капитальные вложения в собственную инфраструктуру. Выходом из сложившейся проблемы может стать реализация

процессов информационной безопасности на сервисной основе, когда программное обеспечение, лицензии, а зачастую и аппаратные средства предоставляются сервис-провайдером в аренду в формате ежемесячной/годовой подписки. Это направление аутсорсинговых услуг носит название MSS (Managed Security Services) и сейчас активно развивается на российском рынке как со стороны компаний-производителей, так и среди крупнейших системных интеграторов и телеком-операторов.

Какая часть технологических задач оперативного уровня при этом закрывается сервис-провайдером? Это напрямую зависит от того, какую задачу безопасности решает предоставляемая технологическая платформа.

• В случае основных сервисов безопасности — межсетевые экраны, VPN, антиспам. Сервис-провайдер со своей стороны только гарантирует работоспособность платформы и зафиксированные в договоре метрики доступности. Но так как данные системы практически не отнимают времени ответственного сотрудника и не требуют специфических компетенций в области ИБ для своей эксплуатации, то большего объема услуг компании не требуется.

• При работе с более кастомизированными сервисами — категориальная фильтрация трафика, контроль приложений, антивирусы. Нередко в базовый пакет услуг включены и работы по администрированию системы, чтобы сократить внутренние расходы компании на ИТ-персонал.

• Если же речь идет о сервисах ИБ, осуществляющих технически сложные процессы, например, о SIEM- или DLP-решениях, зачастую сервис-провайдер готов также предоставлять услуги по частичной реализации сопутствующего системе процесса обеспечения безопасности — мониторинг и реагирование на выявленные утечки/инциденты ИБ.

Такой подход к предоставлению сервисов существенно повышает гибкость рынка услуг информационной безопасности — компания освобождается от риска капитальных вложений в систему, которая через достаточно короткое время не оправдает ее ожиданий. За разумную арендную стоимость она получает возможность детально оценить особенности технологической платформы и использовать опыт и компетенции крупных системных интеграторов в ежедневном процессе обеспечения своей безопасности.

ОПЕРАТИВНЫЙ УРОВЕНЬ – ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ БЕЗОПАСНОСТИ

Но при этом работа службы информационной безопасности не ограничивается эксплуатацией систем ИБ и включает в себя существенный объем организационных мероприятий. Перечислим основные из них:

• ведение и актуализация политик ИБ и сопутствующих им должностных инструкций персонала;

• внутренние аудиты информационной безопасности, направленные на обеспечение и контроль выполнения требований регуляторов, соблюдение внутренних корпоративных политик ИБ, поддержание актуальности существующей информации об их состоянии;

• непосредственная работа с сотрудниками компании, включающая инструктирование и обучение пользователей, внутренние аудиты подразделений для контроля осведомленности о корпоративных политиках безопасности и др.

Эти мероприятия также несут в себе существенную трудоемкость и требуют достаточно специфических квалификаций от сотрудников службы ИБ. При этом они должны учитывать постоянные изменения в законодательстве и предписаниях регулирующих органов, специфику работы различных подразделений и решаемых ими задач, новые угрозы и сценарии нарушения и обхода корпоративных политик. Поэтому резонно рассматривать передачу этих задач в руки внешней компании, специализирующейся на такой активности и использующей свои навыки, являющиеся аккумулированным опытом проведения аналогичных мероприятий в других организациях.

Отметим, что все описанные задачи могут функционировать в компании как в условно непрерывном режиме, когда эти работы являются частью ежедневной активности службы ИБ, так и выполняться на регулярной основе согласно заранее согласованному и спланированному графику. Можно ли во втором случае говорить об аутсорсинге? Да, если данные работы компания доверяет одному и тому же подрядчику на системной основе и не привлекает сторонние ресурсы для их реализации.

ТАКТИЧЕСКИЙ УРОВЕНЬ – СОПРОВОЖДЕНИЕ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИБ

Все описанные выше задачи являются должностными обязанностями и ответственностью обычных сотрудников службы ИБ и связаны с поддержанием и внутренним совершенствованием текущего уровня защищенности. Но этих, безусловно, нужных мероприятий недостаточно для качественного роста и систематизации состояния информационной безопасности. Контроль общего процесса ИБ является задачей руководителя подразделения информационной

безопасности и включает в себя в том числе:

• анализ рисков ИБ и обоснование необходимых изменений в структуре обеспечения безопасности перед руководством компании;

• развитие и совершенствование применяемых в компании средств защиты и систем ИБ, в том числе принятие решений о необходимости расширения их состава;

• внутренний контроль службы ИБ и внешних подрядчиков, оказывающих подобные услуги;

• проверка надежности применяемых в компании защитных мер для реализации нормативных и корпоративных требований по ИБ.

Аутсорсер может взять часть операций в перечисленных процессах на себя, например, если говорить об управлении рисками ИБ, он может обеспечивать инвентаризацию активов, определение их уязвимостей и связанных угроз, а также расчет уровня риска по имеющейся в компании методике. При этом аутсорсер без привлечения представителей заказчика (в частности бизнес-подразделений и высшего руководства) не сможет определить ущерб от реализации тех или иных угроз, а также приемлемый уровень риска. Если говорить о внутреннем контроле безопасности, то партнер может выявить проблемы и несоответствия, дать рекомендации по устранению их причин, но конечное решение (в том числе связанное с выделением дополнительных ресурсов) должна принимать компания. В этом случае интегратор выступает в роли рук для сбора и агрегации информации по различным аспектам ИБ, а заказчик принимает окончательные решения по изменению процессов и мер обеспечения ИБ.

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

За границей нашего рассмотрения остался последний, самый высокий и критичный уровень обеспечения безопасности. Безусловно, идея передачи всей непрофильной для компании активности по ИБ в надежные руки может выглядеть привлекательно и вызывать интерес у некоторых организаций. Но передача сопутствующей ответственности за принятие решений, бюджетирование и развитие информационной безопасности, включая продвижение этого направления в глазах высшего руководства, не выглядит оправданной мерой. При этом на текущий момент на российском рынке не существует компаний, готовых оказывать услуги подобного рода с полноценной финансовой и репутационной ответственностью за результаты своей работы. Поэтому говорить об аутсорсинге стратегического уровня информационной безопасности пока преждевременно.

• • •

Как можно видеть, вариативность услуг по аутсорсингу ИБ достаточно велика. Она позволяет как сократить прямые или сопутствующие расходы на персонал службы информационной безопасности, занимающийся технической эксплуатацией систем ИБ или организационными мероприятиями, так и получать экспертно-аналитические услуги по ежедневному сопровождению критичных процессов обеспечения безопасности или управлению ИБ. Главное — определить самые актуальные и сложные для компании задачи информационной безопасности и выбрать надежного сервис-провайдера. JI

ПРОЦЕССЫ РАЗНЫЕ НУЖНЫ, ПРОЦЕССЫ РАЗНЫЕ ВАЖНЫ

Действовать без правил – самое трудное и самое утомительное занятие на этом свете.

А. Мандзони (1785–1873)

АННА КОСТИНА,
руководитель направления систем управления безопасностью Центра информационной безопасности компании «Инфосистемы Джет»

ПРОЦЕССЫ РАЗНЫЕ НУЖНЫ...

Тема управления инцидентами и менеджмента ИБ в целом обсуждается на протяжении многих лет. Однако нечасто можно увидеть в компаниях зрелые процессы управления ИБ. К сожалению, организационным аспектам информационной безопасности не уделяется достаточно внимания. Видимо, из-за устоявшегося мнения о низкой эффективности таких организационных мер и необходимости внедрения технических мер при желании повышения эффективности обеспечения ИБ.

Да, технологии шагнули достаточно далеко, теперь мы имеем дело с системами, которые умеют собирать всевозможные события ИБ,

Политики информационной безопасности или внедренные меры по ИБ сами по себе не гарантируют защиты информации, информационных систем, сервисов и сетей. После внедрения мер обеспечения ИБ всегда имеют место остаточные риски. Вследствие чего вероятно возникновение событий и инцидентов информационной безопасности, которые потенциально могут иметь как прямое, так и косвенное негативное влияние на бизнес организации. Также всегда существует вероятность реализации новых, не известных до настоящего времени угроз ИБ.

Неготовность организаций к реагированию на подобного рода ситуации может существенно затруднить восстановление нормального функционирования бизнес-процессов и усилить нанесенный ущерб. Таким образом, любой компании, серьезно относящейся к вопросам обеспечения информационной безопасности, необходимо реализовать комплексный подход для решения следующих задач:

- обнаружения, информирования об инцидентах информационной безопасности и их учета;
- реагирования на инциденты информационной безопасности, включая применение необходимых средств для предотвращения, уменьшения и восстановления после нанесенного ущерба;
- оповещения об уязвимостях, которые могут вызвать события ИБ и, возможно, инциденты ИБ, их оценки и должной обработки;
- обучения на инцидентах ИБ, планирования превентивных мер защиты и улучшения процесса обеспечения информационной безопасности в целом.

Именно так начинается стандарт по управлению инцидентами ИБ ISO/IEC 27035:2011. По сути, эта краткая преамбула стандарта говорит нам о необходимости выстраивания полноценного процесса управления инцидентами.

агрегировать и коррелировать их. Но одних систем мало. На основании каких данных и по каким критериям можно определить, имеем ли мы дело с событием или уже с инцидентом ИБ? Что делать после того, как были выявлены критичные события ИБ, которые могут сигнализировать об инциденте? Кому и как передать его на разрешение? А если произошло несколько инцидентов, за какой из них хвататься первым?

Ответить на эти вопросы в короткие сроки может только выстроенный зрелый процесс управления инцидентами ИБ. Без него использование даже самых современных систем мониторинга событий информационной безопасности может свести весь эффект, ожидаемый от их внедрения, на нет.

При построении процесса управления инцидентами ИБ наиболее важно продумать следующие аспекты:

- понятие инцидента ИБ именно для вашей организации. Это, пожалуй, краеугольный камень в строительстве процесса управления инцидентами ИБ. Так, например, для одних организаций внешнее подключение к критичным серверам для изменения файлов — инцидент высочайшей критичности, а для других, у которых оборудование находится на аутсорсинге, такие подключения — норма жизни;
- способы получения сведений о событиях ИБ. Здесь важно определить средства, которые позволят собирать информацию о событиях, а также непосредственно источники данных о них;
- классификация инцидентов как по типам, так и по степени критичности. Именно классификация по критичности позволит правильно расставить приоритеты при разрешении инцидентов ИБ. А классификация по типам поможет правильно определить состав участников для группы реагирования и разрешения инцидента ИБ;
- путь передачи инцидента ИБ на разрешение. Для различных типов инцидентов необходимо определить ответственных или группы ответственных за их разрешение. Немаловажно определить способы и порядок их оповещения об инциденте;
- порядок проведения анализа причин возникновения инцидентов. Этот аспект как раз относит-

ся к тому самому обучению на инцидентах, о котором нам говорят практически все стандарты и рекомендации по этому процессу. Необходимо определять причины инцидентов ИБ для предотвращения их появления в будущем.

Все, что описано выше, стало уже прописными истинами, когда говорят об управлении инцидентами информационной безопасности. Однако, несмотря на это, достаточно большое количество компаний внедряет дорогостоящие средства мониторинга событий ИБ, при этом не заботясь о построении процесса «вокруг» внедряемого решения, и через некоторое время разочаровывается в закупленной системе, т.к. сама по себе она не может обеспечить полноценное управление инцидентами ИБ.

...ПРОЦЕССЫ РАЗНЫЕ ВАЖНЫ

Неготовность и нежелание выстраивать процессы управления инцидентами ИБ или их незрелость до недавнего времени не сулили ничего, кроме локальных проблем в рамках отдельно взятых организаций. Однако сейчас, когда компании начинают все чаще задумываться о передаче процессов обеспечения и управления информационной безопасностью на аутсорсинг, непонимание необходимости педантичного выстраивания процессов может сыграть злую шутку со всеми участниками этого взаимодействия.

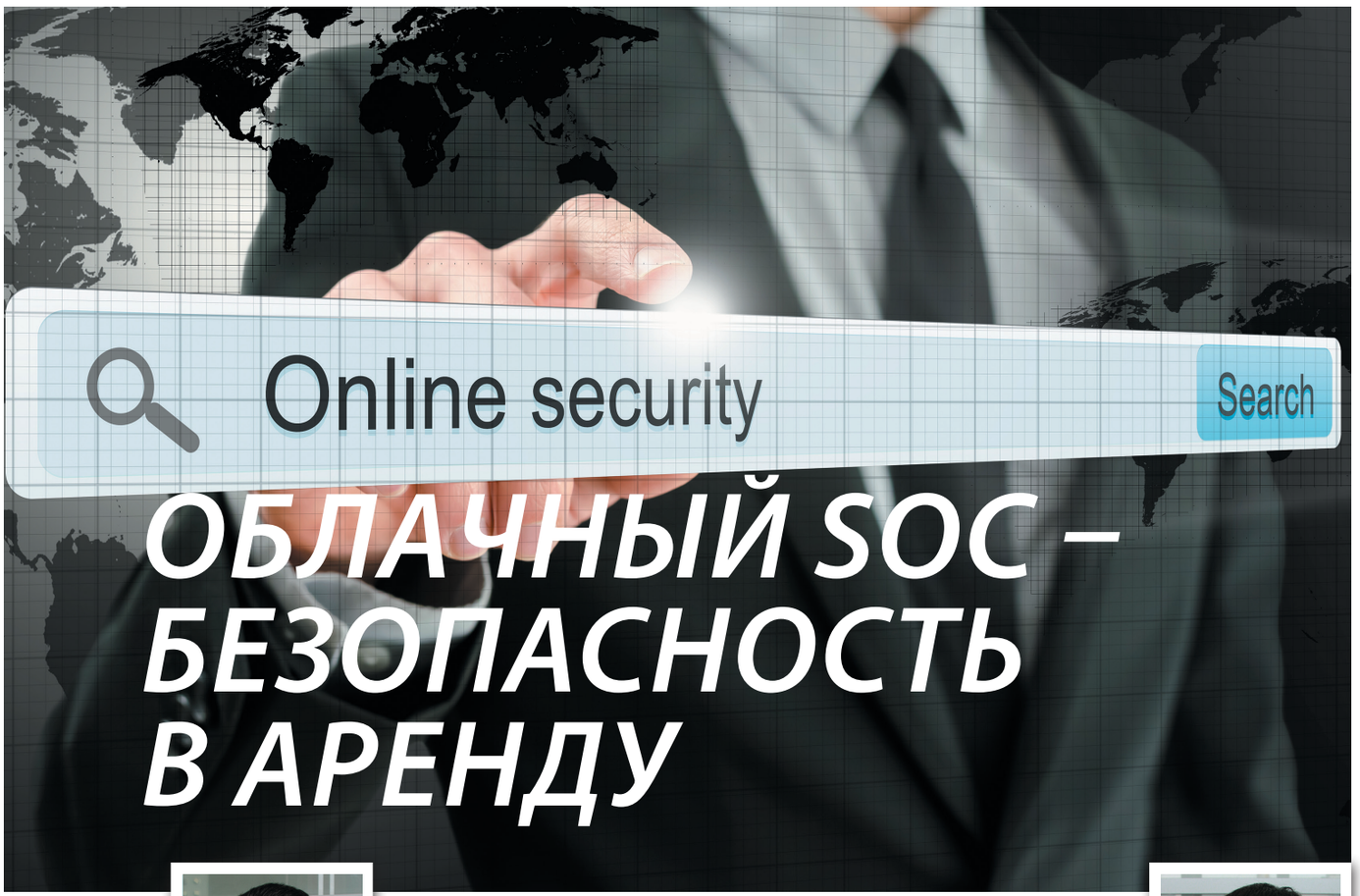
Если раньше в рамках процесса управления инцидентами ИБ требовалось организовать взаимодействие между собственными подразделениями, то теперь необходимо организовать его с внешней компанией, разделить функции и ответственность.

Организациям, которые уже имели дело с процессом управления инцидентами ИБ, в этом плане будет гораздо проще. А что делать тем, у которых его не было?

Анализируя обсуждения рынка аутсорсинга (не только информационной безопасности), мы можем констатировать, что часто встречаются ситуации, когда организации, передавая на аутсорсинг какие-либо процессы или функции, считают, что, переложив их на аутсорсера, они могут не принимать никакого дальнейшего участия в управлении переданным процессом.

И это опасный подход, особенно если говорить о процессах информационной безопасности. Аутсорсер даже при большом желании и высоком профессионализме не может полностью забрать себе процессы ИБ заказчика. На его стороне будут реагирование, технологическое разрешение и анализ инцидентов, их техническое расследование. Аутсорсер может выдать рекомендации о том, что необходимо поменять, чтобы предотвратить появление определенных инцидентов в будущем. Однако конечное принятие решения по внедрению мероприятий по предотвращению инцидентов ИБ, снижению ущерба от них в любом случае остается на стороне заказчика.

Именно поэтому жизненно важно выстроить порядок взаимоотношений между компанией и аутсорсером, определить пороги и границы. Т.е. установить те самые правила, которые позволят сделать процесс управления инцидентами из «самого трудного и утомительного занятия на свете» полезным и эффективным. Выстраивание процесса в аутсорсинговой модели почти ничем не отличается от его выстраивания в рамках одной компании. Все те же аспекты, которые требуют внимания. Однако еще большее внимание требуется уделить распределению ответственности. Но, решив эти вопросы и выстроив процесс управления инцидентами ИБ и взаимодействие с аутсорсером, можно получить эффективную «машину» для их управления и все выгоды от использования этого процесса. В частности, возможность предотвращения или существенного снижения ущербов (как финансовых, так и репутационных) от инцидентов ИБ, повышение доверия со стороны клиентов и партнеров, глубокое понимание актуальных для компании угроз, повышение общего уровня защищенности организации. JI



ОБЛАЧНЫЙ SOC – БЕЗОПАСНОСТЬ В АРЕНДУ

ЭЛЬМАН БЕЙБУТОВ,
руководитель направления защиты баз данных и SOC компании «Инфосистемы Джет»

ВЛАДИМИР ДРЮКОВ,
руководитель направления аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет»

На текущий момент о задаче управления инцидентами ИБ уже сказано очень много, и каждая крупная компания реализовала ее или сделала 1–2 подхода к построению этого процесса. Но как театр не заканчивается вешалкой, так и жизнь процесса не завершается его построением. В этой статье мы рассмотрим основные проблемы, с которыми сталкиваются компании в рамках процесса управления инцидентами ИБ, а также разные варианты их решения.

Как правило, первой задачей является автоматизация процесса выявления инцидентов информационной безопасности. На текущий момент на рынке существует большое количество различных SIEM-решений (Security Information and Event Management), которые прекрасно справляются с ней. Но каждое из них требует серьезных стартовых вложений – необходимы закупка оборудования и ПО, привлечение интегратора для обследования инфраструктуры и кастомизации SIEM под конкретные требования бизнеса и службы безопасности. Поскольку суммарная стоимость решения измеряется сотнями тысяч долларов, даже в крупных компаниях зачастую встает вопрос о возможности выделения таких бюджетов.

Но даже если задача создания SIEM-системы решается успеш-

но, на этом построение процесса управления инцидентами ИБ только начинается. Вторым важным аспектом является обеспечение мониторинга и реагирования на возникающие инциденты. Причем в случае, если к SIEM подключены критичные бизнес-приложения или онлайн-сервисы компании, мониторинг и реагирование должны осуществляться в круглосуточном режиме с очень высокой скоростью реакции на возникновение инцидента. Решение по выделению специальной дежурной смены, особенно для работы 24*7, редко проходит проверку финансовой целесообразностью. Каким же образом решается эта проблема?

Самый популярный вариант — использование существующих ресурсов подразделения информационной безопасности. Но сотрудники отдела ИБ имеют большое количество других профильных задач и обычно не могут полноценно обеспечивать требуемую реакцию на инциденты. Совещание/выход на обед/глубокое погружение в разработку организационных мер выдергивают сотрудника из процесса полноценного мониторинга. О режиме 24*7 и говорить не приходится — отделы ИБ, как правило, не имеют круглосуточной дежурной смены. А по странным жизненным законам самый критичный инцидент обязательно произойдет в пятницу поздно вечером, когда сотрудники разошлись по домам, или во время обеденного перерыва. Безусловно, при дальнейшем «разборе полетов» будет найден ответственный, которого накажут по всей строгости. Но инцидент уже произошел, и самое горячее время, когда его последствия можно было минимизировать, упущено.

Вторым вариантом, как правило, становится передача части функций по управлению инцидентами (например, мониторинг и первичное реагирование) в ИТ-подразделение компании, которое зачастую работают в режиме 24*7. Но и здесь не обходится без «подводных камней». Сотрудники ИТ-службы нередко очень далеки от задач ИБ и могут допустить ошибку в определении важности инцидента. Кроме того, им вряд ли по силам полноценно выполнить задачи по определению его источника, причин и провести расследование. При этом ИТ-подразделение само по себе является одной из основных точек контроля в процессе обеспечения информационной безопасности из-за своих повышенных знаний об инфраструктуре и привилегий по работе с ключевыми системами. Поэтому использование их ресурсов для мониторинга ИБ не всегда дает объективные результаты.

Но даже когда, казалось бы, все проблемы решены и процесс управления инцидентами ИБ запущен, остается немаловажный вопрос развития системы. Профили внешних и внутренних угроз ИБ меняются регулярно, а процесс управления инцидентами должен идти в ногу со временем. Сотрудникам ИБ, работающим в рамках конкретной компании, очень сложно выполнять эту задачу: при эксплуатации процессов обеспечения глаза замыливаются, и работа в рамках одной инфраструктуры и компании редко дает пространство для изысканий и исследований в области ИБ.

PRO БЕЗ CONTRA

В связи с этим российские компании начинают задумываться о передаче процесса управления инцидентами на аутсорсинг или получении этого сервиса на облачной основе. Подобные программы достаточно давно существуют и успешно функционируют в Европе и Америке. В числе клиентов MSSP (Managed Security Service Provider) — несколько тысяч компаний, причем эти услуги имеют спрос не только в SMB-секторе, но и у таких гигантов, как Vodafone и T-Mobile. Давайте разберемся, какие из описанных выше проблем можно решить подобным образом.

Во-первых, использование облачного сервиса может избавить от необходимости стартовых капитальных вложений, например в том случае, когда оборудование и ПО предоставляются аутсорсинговой компанией в аренду. Высокая стартовая цена SIEM-решения преобразуется в существенно меньшие ежемесячные платежи. Помимо этого, сервис-провайдер берет на себя обязанности по размещению основного оборудования и гарантирует его доступность и работоспособность в рамках SLA. Он обеспечивает высокую доступность предоставляемой системы, своевременное и корректное проведение всех работ по ее администрированию и сопровождению, квалифицированное и быстрое предоставление информации из нее. Таким образом, со службы ИБ снимается нагрузка, позволяя ей заниматься другими, не менее приоритетными, задачами по обеспечению безопасности компании. При этом величина регулярных платежей, представляющаяся достаточно высокой при первом рассмотрении, становится более понятной и обоснованной, если учесть косвенные расходы, начиная с уплотнения серверного помещения и обеспечения электропитания до налоговых и премиальных выплат, работы руководителей и кадровых служб, которые получат дополнительную нагрузку (мы не говорим о затратах на закупку оборудования, лицензий и расширение зарплатного фонда).

Во-вторых, внешний сервис-провайдер готов оказывать услуги по мониторингу и реагированию на инциденты в выбранном компанией режиме с теми метриками и набором услуг, которые ей необходимы. В случае, если целевой задачей является мониторинг состояния и защищенности критичного онлайн-сервиса (угрозы несанкционированного доступа, изменения конфигураций, атак на приложение), то контроль, безусловно, должен осуществляться в круглосуточном режиме, а время выявления и оповещения о возникшем инциденте ИБ — измеряться минутами. Но при этом сам процесс расследования инцидента требует крайне ограниченного объема информации, а задачи по реагированию и противодействию могут быть целиком решены сотрудниками, обслуживающими сервис.

Если же речь идет о выявлении и устранении сетевых аномалий инфраструктуры, контроле непрофильного использования технологических систем и учетных записей или анализе интернет-активности пользователей, то критичность такого рода инцидентов чаще всего ниже. Это снижает требования компании к временным показателям услуги, но существенно влияет на объем проводимого анализа и периодически требует активного участия сервис-провайдера в противодействии инциденту и устранении его последствий. Поэтому формирование SLA важно для получения нужного набора услуг с необходимыми метриками обслуживания.

В-третьих, опытный сервис-провайдер, помимо консалтинговой составляющей, обладает экспертизой в интеграции облачного сервиса с банковскими системами, оборудованием связи телеком-операторов, системами управления технологическими процессами, а также CRM- и ERP-приложениями. Это позволяет построить процесс управления инцидентами ИБ, максимально приближенный к задачам обеспечения безопасности бизнес-систем, а не только общей инфраструктуры.

Накопление и использование опыта других компаний, получающих аналогичные услуги, позволяет более глубоко и системно подходить к сценариям определения инцидентов. Последние тенденции отрасли и изменение профилей угроз — новые банковские стандарты безопасности, контроль выполнения требований регуляторов по защите персональных данных или активная борьба с веб-угрозами и DDoS-атаками в публичных сегментах инфраструктуры — также находят отражение в предоставляемой сервис-провайдером базе инцидентов.

При подключении компаний к облачным сервисам проводится адаптация разработанных процедур и уточняется формат оказания услуги по следующим направлениям:

- обследование инфраструктуры и выявление состава подключаемых источников;
- формирование перечня журналируемых событий;
- кастомизация общей базы контролируемых инцидентов под задачи и потребности компании, их приоретизация;
- определение ролей сотрудников, участвующих в расследовании инцидентов;
- согласование порядка и способов взаимодействия при расследовании инцидентов в зависимости от их типа и критичности;
- подготовка и планирование проактивных мер ИБ, предотвращающих повторное возникновение инцидента.

Причем процесс формирования перечня событий, не имеющий высокой степени критичности при построении внутреннего SOC, приобретает совсем другое значение в облачном варианте. Даже при соответствующих соглашениях конфиденциальности компания чаще всего не готова транслировать во внешнюю систему не подлежащие разглашению данные. Но на деле для корректного функционирования и выявления инцидентов SIEM достаточно обрабатывать события аудита и общую информацию активности пользователей: фиксируется факт доступа к критичному файлу или таблице базы данных, а не сам файл или информация из БД. Поэтому степень критичности транслируемой информации мало отличается от характера данных, получаемых интегратором при обследовании системы или ее технической поддержке.

Использование процессного подхода, описанного выше, делает реагирование и разрешение инцидентов ИБ более оперативным и позволяет использовать как аккумулированный провайдером, так и собственный опыт компаний по расследованию инцидентов, специфичных для их бизнеса или особенностей инфраструктуры.

• • •

В случае, если компания готова вступить в аутсорсинговые отношения в области управления инцидентами ИБ, следующим ее шагом становится выбор сервис-провайдера, которому она готова доверить этот непростой и важный процесс. В данном случае взаимное терпение в преодолении сложностей на старте, как правило, оказывается более важным, чем скрупулезное согласование состава услуг и метрик обслуживания, и является одним из ключевых факторов успешного взаимодействия. JI

DLP КАК СЕРВИС – МАЛЕНЬКИЕ РАДОСТИ РЕАЛИЗАЦИИ

– Слушай, Гена, давай я понесу чемоданы, а ты понесёшь меня…
– Это ты здорово придумал, Чебурашка!

Мультфильм «Чебурашка и крокодил Гена»

ВЛАДИМИР ДРЮКОВ,
руководитель направления аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет»

ДМИТРИЙ МИХЕЕВ,
эксперт Центра информационной безопасности компании «Инфосистемы Джет»

Тематика контроля утечек конфиденциальной информации является одной из самых популярных в сфере ИБ. Как минимум, контроль утечек — это круто. Вне зависимости от размера и специализации компании в результате своей работы она создает или использует информацию, бесконтрольное распространение которой является крайне критичным риском. Это может быть финансовая информация, данные клиентов и поставщиков, исходный код, разработанный специалистами компании, или другие материалы, например, макеты календарей, веб-сайтов и т.д.

Если данные станут доступны конкурентам или появятся в публичном доступе, это может повлечь за собой прямые финансовые потери компании, очевидные легальные, а также репутационные риски, которые иногда могут оказаться даже более значительными, чем финансовые. Обнаружить, предотвратить актуальные утечки, расследовать факты прошлых инцидентов — это те возможности, которые дают офицеру

ИБ уверенность в сегодняшнем и завтрашнем днях.

При принятии решения об использовании в компании DLP-платформы стоит обратить внимание на некоторые факторы. DLP-система — это, как правило, дорогое удовольствие. Стоимость лицензий, мощностей будет тем более заметна, чем глубже мы хотим изучать потоки информации и чем большим количеством данных компания обменивается с внешним миром.

Серьезные затраты также приходятся на сам процесс внедрения системы: разработка регламентов и политик для ее использования в компании может потребовать ресурсов и некоторого опыта. Внедрение занимает время. Переход от пассивного мониторинга событий к активному противодействию утечкам может легко превысить полгода, не считая затрат на подготовительные работы и согласование у заинтересованных лиц внутри компании. Стоимость оборудования, его размещения и обслуживания, обеспечение квалифицированными кадрами на продолжительный период также являются значительными статьями расходов.

В этой связи идея получить DLP-систему как сервис становится, как минимум, финансово интересной. Целью нашей статьи является попытка проанализировать технические и организационные аспекты вариантов такой реализации и оценить потенциальную эффективность сервисного подхода к эксплуатации DLP-решений.

Одним из возможных вариантов снижения затрат на оборудование и лицензии является получение их на арендной основе или по подписке у производителя или крупного сервис-провайдера. Располагаться система может как на площадке заказчика, так и в собственном облаке поставщика услуги. Классическая архитектура DLP-решения включает следующие стандартные компоненты:

- агенты рабочих станций и серверов, собирающих с этих источников информацию об активности с конфиденциальными данными;
- сенсоры сбора данных, как выступающие в роли точки централизованного сбора информации с агентов, так и собирающие и обрабатывающие ее на сетевом уровне (SPAN-порт, почтовый и веб-трафик);
- узел сбора инцидентов и исторический архив хранения, редактор политики.

Могут ли сенсоры сбора данных быть вынесены с площадки компании в облако? Да, но нужно учитывать ограничения такого подхода. Даже для средней компании объем трафика, поступающего на сенсоры непосредственно с инфраструктуры или с агентов, может быть значительным, поэтому размещение сенсоров DLP в облаке потребует увеличения полосы пропускания внешних каналов связи.

Реальным вариантом реализации такого подхода является получение сервиса контроля утечек непосредственно от провайдера каналов связи и сбор требуемых данных в «трубе» интернет-соединения. В принципе, для начала этого может быть достаточно. Но эта схема оставляет за скобками обеспечение контроля наиболее любопытных каналов утечки информации — рабочих станций, съемных носителей, шифрованных интернет-сессий и файловых серверов.

Таким образом, агенты и сенсоры сбора событий в большинстве случаев должны быть расположены на собственной площадке компании, а в облаке сервис-провайдера могут быть размещены архив инцидентов и редактор политики. При этом немаловажными вопросами становятся критерии сохранения событий и его максимальные сроки — в случае необходимости долгого хранения всей или большой части исходных событий мы неизбежно сталкиваемся все с той же проблемой нагрузки на интернет-каналы, а также со стоимостью архивирования значительных объемов информации.

Помимо самой технической возможности хранения в облаке стоит проанализировать, что именно в него попадает. В случае DLP-платформы речь идет о целевом хранении всех транзакций конфиденциальных данных за пределами компании — заметной части почтовой переписки, интернет-активности пользователей и результатов обработки файлов на рабочих станциях (передачи на съемные носители или в печать). Для обеспечения защиты от ранее не фиксировавшихся инцидентов существующие DLP-системы предоставляют возможность хранения обширных архивов событий. Полученное хранилище данных по своему содержимому вполне сопоставимо с почтовыми серверами компании, и размещение такого архива в облаке практически аналогично решению по использованию облачных сервисов электронной почты или документооборота. Но далеко не каждая компания готова пойти на это, так как требуется серьезный уровень доверия к поставщику подобной услуги. Стоимость решения будет заметной, хотя и дешевле по сравнению с тем, если бы организация сама купила оборудование, лицензии и обеспечила ресурсы ЦОД.

Тем не менее, несмотря на эти очевидные вопросы, интерес к подобному варианту использования DLP-системы сохраняется. Есть примеры, когда компании реализуют вынос обработки событий в собственные, принадлежащие им облака во внешних ЦОД, от такой схемы остается только один шаг до перехода на сервисную модель.

Можно резюмировать, что вопрос использования DLP-платформы на облачной основе несет в себе заметный набор технических и организационных рисков, тем самым делая его применимым далеко не для каждой организации и не во всяком случае. Но даже в случае приобретения самой платформы компания имеет возможность существенно сократить свои расходы на ее дальнейшее обслуживание за счет привлечения сервис-провайдера для обеспечения самого процесса контроля утечек. Если изначально для контроля бизнес-информации достаточно ограниченного набора каналов (например, события обмена с внешними сервисами), выбор облачного варианта использования уже можно рассматривать.

ЕСТЬ ЛИ МЕСТО ИНТЕГРАТОРУ?

Для того чтобы проанализировать потенциальную полезность сервис-провайдера в обеспечении процесса контроля утечек конфиденциальной информации, необходимо разложить на составляющие сам процесс обработки утечки, зафиксированной системой. Его можно разделить на следующие этапы:

- реализация политики безопасности — разработка и отладка правил автоматического реагирования на события для системы;
- выявление инцидента — активный мониторинг событий, зарегистрированных в системе, фактическое обнаружение и фиксация инцидента;
- разбор инцидента — отсечение ошибок первого рода или ложных срабатываний, уточнение его критичности, эскалация факта возникновения инцидента (при необходимости);
- анализ инцидента — определение его источника (в данном случае речь чаще всего идет о конкретном сотруднике компании), причины возникновения (например, недостаточно жесткая политика блокирования веб-трафика или нарушения в бизнес-процессах), анализ сопутствующей активности пользователя в момент возникновения утечки, эскалация на соответствующие подразделения;
- блокирование инцидента — активное техническое противодействие произошедшей утечке и возможности ее повторения;
- дальнейшее расследование инцидента — коммуникация с пользователем, его непосредственным руководителем и внутренней службой безопасности и прочие нетехнические способы получе-

ния и обработки информации о пользователе и инциденте.

Крайне редко компания готова предоставить сервис-провайдеру доступ для просмотра и анализа исходных событий утечки (тела электронного письма, файла, передаваемого на флеш-носитель), поскольку данная информация имеет очень высокий уровень конфиденциальности и не может быть передана для анализа сторонней организации даже при соответствующем уровне соглашений. Поэтому популярным сценарием вовлечения сервис-провайдера является делегирование ему частичных прав на исходные события: с маскированием или шифрованием исходной информации, с предоставлением только общих данных о структуре утечки, названиях файлов, их размере и т.д.

Какие из описанных этапов расследования при таком подходе может полноценно выполнять партнер? Первичный разбор инцидентов — это основной сценарий. Такой подход позволяет снять нагрузку с офицеров безопасности, при этом оставляя возможность контроля над ситуацией.

Варианты привлечения сотрудников интегратора также имеет смысл рассмотреть, если параллельно оказываются прочие услуги по безопасности — анализ событий, учет уязвимостей и т.п. Еще одним хорошим сценарием может являться организация на площадке поставщика услуги выделенного узла защиты интернет-коммуникаций для компании — комплексного решения по защите входящих данных от спама, malware, phishing и других подобных рисков, дополненного DLP-средствами для исходящих данных.

Для самого факта фиксации срабатывания правил системы и регистрации инцидента не требуется высокого уровня доступа и анализа информации. В процессе более глубокого анализа инцидента уже могут возникать сложности. Провести корректное отсечение ошибок второго рода достаточно сложно, если не иметь доступа к исходному сообщению, особенно в случаях, когда политики выявления базируются не на простых высоковероятных событиях (ключевые слова, регулярные выражения или умные идентификаторы, такие как номер кредитной карты, паспорта и социального страхования), а требуют детального анализа текста, например, с использованием технологии цифровых отпечатков.

При этом одной из наиболее оптимальных является схема совместной ответственности за этап: сервис-провайдер выполняет разбор инцидента самостоятельно для простых правил срабатывания или тогда, когда вероятность совпадения файла с цифровым отпечатком близка к 100%, в противном случае запрашивает дополнительную информацию по исходному сообщению у ответственного специалиста компании или передает ему разбор инцидента целиком. Безусловно, при этом оба участника процесса серьезно зависят от возможностей и качества работы используемой программной платформы: если внутренние алгоритмы системы или реализуемые политики допускают высокую погрешность в результате, достаточно сложно выстроить комфортное для обеих сторон взаимодействие.

В процессе рассмотрения и блокирования инцидента роль сервис-провайдера может быть достаточно существенной: и оценка политик вместе с разработкой инструкций по их ужесточению или оптимизации, и ретроспективный анализ событий зачастую требуют не непосредственного доступа к конфиденциальной информации, а достаточно высоких компетенций относительно анализа данных, современных способов организации утечек и применяемых средств защиты. При этом принятие решения о применении политик блокирования и сам процесс дальнейшего расследования инцидента остаются на стороне компании и вряд ли могут быть переданы интегратору.

Более глубокие методы взаимодействия с накопленным архивом инцидента, например, с использованием возможностей интеллектуального поиска невыявленных инцидентов по историческому архиву сообщений, находятся уже за пределами доступа специалистов интегратора. Данная аналитическая задача требует максимального уровня доступа к информации и чаще всего остается в зоне ответственности компании. Интегратор может выступать как консультант по наилучшим практикам и возможностям системы, не имея непосредственного доступа к данным.

• • •

В итоге при должных функциональных возможностях системы DLP (ролевое управление и маскирование данных, возможность работы с частично обезличенной информацией) вполне можно реализовать схемы совместного сопровождения процесса контроля утечек для компании и ее партнера, причем с финансовой выгодой по сравнению с полным владением DLP-решением. При этом компания может осуществлять данный процесс в круглосуточном режиме без значительных расходов на организацию дежурной смены и существенно сократить нагрузку на существующих специалистов, передав рутинные и трудоемкие задачи интегратору. JI

© Кадр из фильма «Хакеры»

Один день из жизни Ричарда Джилла, специального агента секретной службы США, превратился в кошмар наяву. У него аннулировали банковские карты, отобрали права и эвакуировали автомобиль за многочисленные грубые нарушения правил дорожного движения, а ближе к вечеру он и вовсе обнаружил, что числится умершим в системе кадрового учета своего ведомства. Все дело в том, что на него буквально устроили охоту хакеры из одноименного фильма. Несмотря на то что картина вышла в середине 1990-х, этот эпизод по своим характеристикам является прообразом современных APT-атак – Advanced Persistent Threat. Тот же предварительный сбор данных об объекте, распределение ролей между атакующими, полный контроль над жертвой, наблюдение за ней в режиме реального времени. Остается только один вопрос – как защититься от APT? Сегодня мы говорим о причинах и последствиях такого рода атак, а также технологиях противостояния им с ***Борисом Симисом, заместителем генерального директора компании Positive Technologies.***

J.I.: Борис, предлагаем начать с истории вопроса. Откуда есмь пошел термин APT?

Б.С.: Его ввели в 2006 году Военно-воздушные силы США для обозначения атак, длящихся долгое время и характеризующихся мощными векторами. Естественно, подобные инциденты были и до этого: целевые атаки на крупные предприятия через web-сайты, удаленные филиалы и т.д. В определенный момент их просто нарекли APT. Если просмотреть новостные ленты 2008–2009 годов, одна тенденция прослеживается четко: взлом той или иной корпорации будоражил умы, это была, простите за каламбур, информационная бомба. Но за последние 3 года в отношении этой парадигмы атак произошёл переломный момент – успешно реализованные APT уже никого не удивляют. Из разряда событий они перешли в повседневность.

J.I.: Какие самые яркие примеры APT Вы можете вспомнить?

Б.С.: Среди последних масштабных взломов я бы выделил историю с Sony в 2011-м. Началась она годом ранее, когда компания обновила прошивку на своих приставках PlayStation 3. Если раньше пользователи могли устанавливать на них другие ОС, теперь эта возможность исчезла. Хакеры не могли остаться равнодушными к такому ограничению свободы трудящихся. Джордж Хотц «вскрыл» PS3, вернул себе возможность установки сторонних ОС, а заод-

но опубликовал в сети эксплойты, позволяющие другим взломать коды безопасности. Sony отблагодарила парня, подав на него в суд, что не на шутку разозлило интернет-сообщество.

Сеть PlayStation Network за несколько дней была взломана, злоумышленники завладели персональными данными более 80 миллионов пользователей, в том числе информацией об их кредитных картах. Sony понесла прямые убытки — ее акции за ту «черную» неделю упали на 8%. А в этом году британцы обязали компанию еще и штраф уплатить — в том числе пострадали жители Англии. Справедливости ради отмечу, что эта атака по своим признакам не вполне соответствует APT, поскольку последние в своем классическом варианте подразумевают тщательную подготовку, незаметность для жертвы и могут развиваться месяцами.

J.I.: А если говорить о более «образцовых» случаях?

Б.С.: Взлом в 2010 году иранской атомной электростанции «Бушер» высокотехнологичным вирусом Stuxnet, который был разработан израильскими и американскими кибервойсками. Он использовался для срыва работы реальных объектов гражданской инфраструктуры. Программа попала на один из компьютеров АЭС через USB-устройство. Она захватывала все новые машины, пока не добралась до той, на которой стоял софт Siemens, управляющий непосредственно центрифугами, обогащающими уран. Stuxnet изначально был заточен под взлом ПО вендора, его разрабатывали для этой цели. Вирус пытался разрушить двигатели нескольких сотен центрифуг, резко снижая и увеличивая частоты вращения конвертера.

Стоит также назвать взлом компьютерных систем газеты New York Times. Занятно, что именно она установила причастность госхакеров США к APT в Иране. По заявлению издания, на протяжении 4 месяцев китайские кибервойска пытались получить доступ к его компьютерам. В результате 53 ПК все-таки «сдались».

«ИНТЕРНЕТ – ЭТО МИРОВОЙ МЕГАПОЛИС. ОН ОБЪЕДИНИЛ СОВЕРШЕННО РАЗНЫХ ЛЮДЕЙ: КИТАЙСКОГО ХАКЕРА-ИНТЕЛЛЕКТУАЛА, ЗАРАБАТЫВАЮЩЕГО 50$ В МЕСЯЦ, И АМЕРИКАНСКУЮ КОРПОРАЦИЮ С МИЛЛИОНАМИ ДОЛЛАРОВ. И ОБЪЯСНИТЬ ЕМУ «ПОСЛУШАЙ, ВЕДИ СЕБЯ ХОРОШО», ОЧЕНЬ ТЯЖЕЛО. APT РОДИЛОСЬ ИЗ ЭТИХ ПРОТИВОРЕЧИЙ».

J.I.: Вы можете выделить, кто сегодня в наибольшей степени находится под прицелом? Или подобную закономерность нельзя проследить?

Б.С.: В год в России проводятся сотни тестов на проникновение, грубо говоря, идет проверка, насколько легко можно взломать ту или иную компанию. И практика показывает, что перед APT-взломом не выстоит ни финансовая организация, ни телеком-оператор, ни госструктура.

Вопрос, соответственно, — только в целях, которые могут преследовать хакеры. Еще несколько лет назад ломали исключительно ради зарабатывания денег: сеть школы не представляла такого интереса, как базы данных сотовых операторов или персональные данные клиентов банка. Но с 2010–2011 годов на этом «рынке» появились новые силы.

J.I.: Исходя из Ваших примеров APT это в том числе госхакеры.

Б.С.: Да, кибервойска, в том числе пытающиеся получить доступ к промышленным секретам других стран. Поэтому объектами нападения становятся системы городских хозяйств, сегменты гражданской инфраструктуры, остановка которых может привести к нарушению ритма жизни целых регионов. Как вы понимаете, о прямой монетизации в этих случаях речи не идет. Кроме того, на сцену вышли так называемые хактивисты, те же Anonymous, взламывающие по идеологическим соображениям — против загрязнения окружающей среды, притеснения религиозных групп, в защиту прав животных и т.д. Иногда достаточно единственного клича в интернете — «Они вырубают леса», например, чтобы ресурс госструктуры, отвечающей за

«ЦЕЛЕНАПРАВЛЕННЫЕ ДОЛГОВРЕМЕННЫЕ АТАКИ БЫЛИ ВОЗМОЖНЫ ВСЕГДА, НО РАНЬШЕ ЗЛОУМЫШЛЕННИКИ НЕ ВИДЕЛИ В НИХ ОСОБОГО СМЫСЛА, ПОСКОЛЬКУ, ЗА РЕДКИМ ИСКЛЮЧЕНИЕМ, НЕ МОГЛИ МОНЕТИЗИРОВАТЬ ИХ ПОСЛЕДСТВИЯ. СЕГОДНЯ ЦЕЛИ ХАКЕРОВ ИЗМЕНИЛИСЬ, И ПОД ПРИЦЕЛОМ ПОТЕНЦИАЛЬНО НАХОДИТСЯ ЛЮБАЯ ОРГАНИЗАЦИЯ».

лесное хозяйство, подвергся атаке. Одним словом, хактивисты значительно расширили список потенциальных мишеней — теперь от APT никто не застрахован.

Еще один «вектор силы» — взлом ПК и смартфонов обычных пользователей, ставший отдельным бизнес-направлением на «черном» ИТ-рынке. Буквально в марте в США была обнаружена бот-сеть из 120 000 угнанных компьютеров, и это, что называется, нижний порог, сегодня не редкость — сети из миллионов ПК.

J.I.: Как Вы считаете, могут ли компании самостоятельно обеспечить себе необходимый уровень безопасности?

Б.С.: Наше время с точки зрения обеспечения корпоративной ИБ является переломным. С одной стороны, компании располагают огромным количеством средств защиты: антивирусы, межсетевые экраны, мониторинг, чего только нет. С другой, как я уже говорил, практически любую организацию можно взломать. То есть силы APT-атакующих явно преобладают над ресурсами обороняющихся. Современные технологии защиты ограничены — они защищают только от стандартных атак. А хакер-APT-шник, прежде чем написать вирус «в подарок» какой-нибудь компании, определит, сможет ли та зафиксировать его своими средствами. Естественно, вредоносное ПО проскочит. В то же время ИТ-технологии так быстро идут вперед, что безопасникам бывает тяжело за ними угнаться. Мы только разобрались с защитой внешнего периметра, как появляется Bring Your Own Device. Сотрудники хотят пользоваться своими гаджетами для работы в любом месте — какой уж тут периметр.

Исходя из вышесказанного первое, что нужно сделать компаниям, — это признать, что их защита несовершенна. Но российский рынок пока не готов к публичному обсуждению подобных проблем. Возьми любую зарубежную ИБ-конференцию — тема целенаправленных взломов находится в топе. «Нас ломают. Что нам делать?» — так начинаются выступления западных руководителей ИБ-служб. Они вместе ищут решение. У нас же практически все конференции проходят в ключе «построили систему защиты, все функционирует, все нормально».

«Я УВЕРЕН, ЧТО РЫНОК В БЛИЖАЙШИЕ 2 ГОДА ПЕРЕЖИВЕТ РЕИНКАРНАЦИЮ. МНОГИЕ ОСОЗНАЮТ НАЛИЧИЕ ПРОБЛЕМ, И МЫ ПОЛУЧИМ ПРИНЦИПИАЛЬНО НОВЫЕ ПОДХОДЫ К ОБНАРУЖЕНИЮ ВИРУСОВ, РАБОТЕ FIREWALL'ОВ, АНАЛИЗУ ЛОГОВ».

J.I.: Каковы особенности технологий защиты от APT?

Б.С.: Компании, с одной стороны, должны озадачиваться вопросами именно практической безопасности. С другой, ни одна организация не пойдет на создание у себя службы ИБ, которая реально смогла бы противостоять APT. Это, грубо говоря, влетит в копеечку. Необходимы партнеры, специализирующиеся на обеспечении информационной безопасности, обладающие глубокой экспертизой, способные оперативно откликнуться на малейшее подозрение на инцидент и детально разобрать его. Потому как понять, ломают ли тебя сейчас, — это отдельная задача. Как и разобраться с тем, удалась ли хакерам атака. Пример из практики: не так давно проводились исследования защищенности сайтов ряда российских компаний. Каждый 10-й из них взломан, а собственники об этом даже не подозревают.

«МИРОВОЙ ОПЫТ ПОКАЗЫВАЕТ, ЧТО НАИБОЛЕЕ ЭФФЕКТИВНАЯ ЗАЩИТА ОТ APT ВОЗМОЖНА В СЛУЧАЕ ИСПОЛЬЗОВАНИЯ АУТСОРСИНГА».

J.I.: Ваши прогнозы: через несколько лет количество атак только увеличится? Или возможен такой вариант, что хакеры уйдут на пенсию и все успокоятся?

Б.С.: По своей натуре я оптимист, но в данном случае особого повода для веры в счастливый исход дела не вижу. Позволю себе философское отступление: в прошлом году на форуме Positive Hack Days присутствовал криптограф Брюс Шнайер. Он высказал мысль, что мир живет в условиях кризиса привычных механизмов человеческого общежития. Наша жизнь основана на доверии к окружающим людям. В offline мы редко сталкиваемся с мошенниками — раз в полгода-год. Интернет же облегчил доступ огромного числа злоумышленников к объектам своих действий, и градус атак со временем только повышается. Нам нужно либо изменить свою природу и постоянно подозревать окружающих, что маловероятно, либо найти механизмы, которые позволили бы защищать себя принципиально другими способами.

J.I.: Борис, большое спасибо за беседу!

Лавинообразное увеличение объемов передачи данных, ужесточение требований регуляторов по информационной безопасности, аутсорсинг ИБ. Обо всем этом – за или против, реальная тенденция или маркетинговый ход – мы сегодня говорим с ***Евгением Кукушкиным, начальником управления сетевых и серверных технологий ДИТ ДРЦТ ВГТРК.***

J.I.: Какие наиболее критичные риски, связанные с информационной безопасностью, можно указать для сферы электронных СМИ? Есть ли здесь своя специфика, или «все как у всех»?

Е.К.: Прежде всего это несанкционированный доступ к информации, которую еще не увидел свет, – риски утечки. Она может быть разного характера – авторские передачи, новостные сюжеты и т.д., но при этом не должна уйти за пределы 4 стен до часа X. Это специфическая угроза, поскольку круглосуточное производство подобной информации составляет основу бизнеса холдинга.

С другой стороны, существуют риски, связанные с доступностью данных, например, того же медиа-контента на сайте СМИ. Здесь опасность представляют DDoS-атаки. В качестве примера можно привести недавний факт DDoS-атаки на сайт наших коллег, тоже СМИ, его работоспособность удалось восстановить лишь через 6 часов. Поскольку мы являемся крупнейшим российским медиахолдингом, для нас подобные ситуации недопустимы.

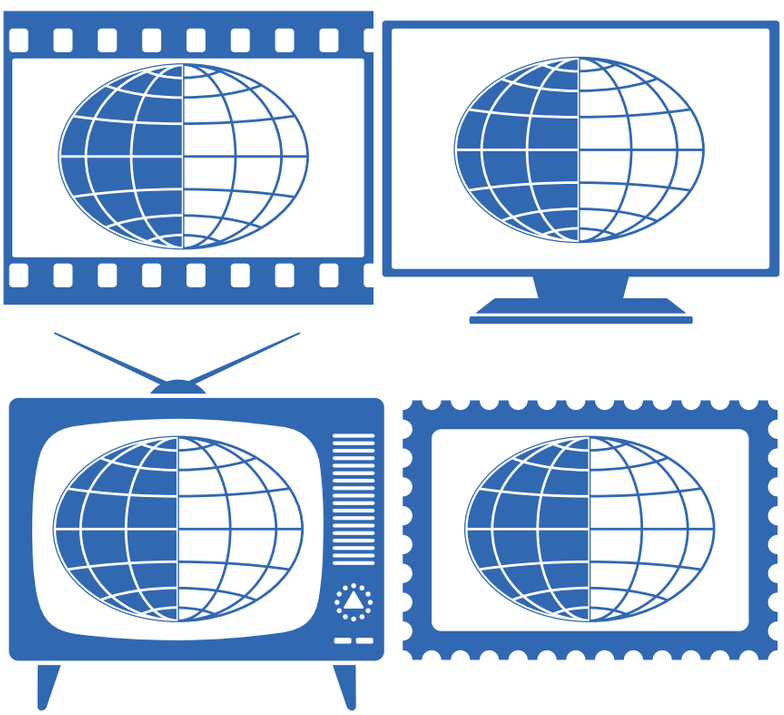
J.I.: Как грамотно выстроить систему защиты в таком случае?

Е.К.: Как вы понимаете, здесь один в поле точно не воин, в любом случае должен быть комплекс мероприятий. Первая линия обороны — физическая безопасность (видеонаблюдение, фиксация перемещения персонала, система контроля и управления физическим доступом). Далее идут программно-технические средства: системы контроля уязвимостей, меры по защите информации в сетях передачи данных, IdM, системы мониторинга событий безопасности и т.д.

J.I.: Какие проекты, касающиеся обеспечения ИБ, были выполнены ВГТРК за последние 2–3 года?

Е.К.: Реализация требований государственных регуляторов по защите персональных данных, построение системы защиты электронной почты (CommuniGate Pro, MS Exchange 2010) с использованием Proofpoint Enterprise Protection for Email Security, создание системы контроля уязвимостей на базе MaxPatrol. В данный момент идет проект по внедрению системы обнаружения и предотвращения вторжений.

Мы не строим иллюзий: как не существует панацеи от всех болезней, так и нет ИБ-решений, обеспечивающих 100%-ную защиту. Здесь вспоминается расхожая фраза: как только политика безопасности окончательно утверждена, она уже окончательно устарела. Это же в определенной степени относится к системам ИБ. Наш бизнес не стоит на месте — увеличиваются потоки посещаемости интернет-ресурсов, растут объем и качество медиа-контента, возрастает сложность взаимодействия между подразделениями компании. В то же время что ни месяц возникают новые угрозы ИБ, которым необходимо эффективно противостоять и желательно действовать превентивно, а не реактивно. Соответственно, постоянно повышаются требования к функционалу решений и к его гибкости.



J.I.: Вы упомянули соответствие рекомендациям наших регуляторов. Ваше мнение — насколько они соотносятся с реалиями российского рынка?

Е.К.: Для себя я представляю это соотношение в виде весов. На одной чаше находятся требования и рекомендации регуляторов, а на другой — ситуация с информационной безопасностью в конкретной компании. Главное — поддерживать разумный баланс. Вынужден констатировать, что если мы выполним досконально все рекомендации (замечу — именно рекомендации, а не требования, которые мы выполняем на 100%), то дальше останется только выключить свет и разойтись по домам — бизнес не сможет нормально функционировать. Конфигурация ИТ-ландшафта будет, мягко скажем, сложноуправляемой.

Проблемой, в том числе, является отсутствие у многих действенных зарубежных решений сертификатов ФСТЭК, а отечественные сертифицированные продукты, к сожалению, не перекрывают весь спектр потребностей компаний.

J.I.: Каким образом на ИТ-инфраструктуру ВГТРК влияет непрекращающийся рост объема данных, характерный для последних лет?

Е.К.: Для начала подчеркну, что растет не только он, но и количество информационных каналов, а также качество медиа-данных. У ВГТРК более 80 региональных филиалов, охватывающих всю страну, многие из них ежедневно

генерируют собственный контент. Естественно, все эти факторы являются двигателями развития.

Исторически региональные ГТРК были самостоятельными единицами — со своими ИТ-ресурсами, архивами аудио и видео. В середине 2000-х годов было принято решение объединить их под одним управляющим центром — отдельно стоящие серверы и системы не могли поддерживать развитие бизнеса на должном уровне. Как вы понимаете, это весьма сложный процесс, занимающий не один год. Мы объединили регионы единой сетью передачи данных, стараясь унифицировать подходы к обработке, хранению, резервированию и защите информации. Другими словами, был сделан ряд необходимых шагов в сторону перехода от локальных, обособленных физических сред к единой корпоративной инфраструктуре, от управления «железом» к управлению ИТ-ресурсами.

Мы как электронное СМИ храним весь свой контент, причем из всех источников его генерации, и параллельно с этим обеспечиваем возможность доступа интернет-пользователей к его части. Для долговременного хранения медиаданных мы создали электронный медиа-архив. Данные хранятся на дисковых и ленточных накопителях (LTO). В проекте используются серверы HP стандартной архитектуры, системы хранения EMC, ленточные накопители Quantum.

J.I.: А объемы данных, о которых идет речь?

Е.К.: На данный момент в архиве у нас порядка 6 тысяч слотов LTO, оцифровано порядка 3 ПБайт информации, но это, как говорят англичане, a drop in the ocean, малая толика. По масштабам проект — один из крупнейших в России.

Также совсем недавно мы провели инсталляцию корпоративной системы резервного копирования на магнитных лентах. Хранилище будет содержать несколько десятков ПБайт информации и управляется роботизированной системой. Она станет частью комплекса иерархического хранения данных (HSM).

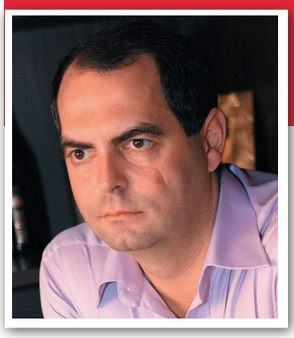
J.I.: Ваше мнение по поводу аутсорсинга, в том числе информационной безопасности, — «за» или «против»?

Е.К.: Есть несколько факторов, влияющих на принятие решения об аутсорсе. Во-первых, «политика партии»: так принято, и по-другому не может быть. Во-вторых, степень зрелости процессов, которые целесообразно было бы передать в руки партнера. Нельзя отдавать на сторону неустоявшиеся процессы, если мы сами не до конца понимаем, как они должны функционировать. С SLA потом костей не соберем. И в-третьих, нужно учитывать степень их критичности.

J.I.: Что в таком случае Вы гипотетически могли бы доверить аутсорсеру?

Е.К.: Если рассматривать информационную безопасность, то можно говорить о системе обнаружения вторжений, обработки и анализа событий ИБ. Если же фокусироваться на ИТ в целом, то это решения по мониторингу, Help Desk, аренда вычислительных мощностей: cloud-среды в любом формате — IaaS, PaaS или SaaS.

J.I.: Евгений, большое спасибо за беседу!



*Тему нашего номера продолжает блиц-интервью с **Юрием Лысенко, начальником Управления информационной безопасности Департамента защиты бизнеса ООО «Хоум Кредит энд Финанс Банк».***

J.I.: Как Вы полагаете, чем является спрос на услуги аутсорсинга ИБ – естественной потребностью, вызванной ростом уровня зрелости процессов обеспечения ИБ в российских компаниях, или искусственно создаваемым интересом к модной нынче теме?

Ю.Л.: Это динамично развивающийся вид оптимизации деятельности подразделений по защите информации. Благодаря ему компания может освободить организационные, финансовые и человеческие ресурсы для развития, а также сконцентрироваться на существующих бизнес-направлениях и проблемах, требующих усиленного внимания. Все это позволяет повысить эффективность ИБ-подразделения в целом, в том числе по тем векторам, где не хватает определенных знаний и нет острой необходимости вкладывать средства, т.к. затраты на развитие превосходят расходы на аутсорсинг.

J.I.: Что является движущей силой аутсорсинга ИБ на российском рынке?

Ю.Л.: Думаю, отсутствие собственных специалистов с определенным уровнем знаний и умений или их неэффективное использование.

J.I.: Для каких компаний (сфера деятельности, масштаб) он актуален?

Ю.Л.: Полагаю, что для организаций Enterprise-уровня, в том числе территориально распределенных, в случае нехватки ресурсов или нецелесообразности привлечения собственных ИБ-специалистов в силу определенной специфики. Для сектора SMB подобные услуги также будут представлять интерес. Скорее, правда, это будет ИТ-аутсорсинг, но в него будут также входить вопросы информационной безопасности.

J.I.: Что целесообразно передавать «на сторону», а что лучше оставить у себя? По каким причинам?

Ю.Л.: Теоретически отдать можно все, но на практике руководство компании вряд ли доверит аутсорсеру, например, контроль за утечками информации или мониторинг действий пользователей в информационных системах. Эти данные сложны в обработке и являются весьма критичными, чтобы допустить к ним сторонних лиц.

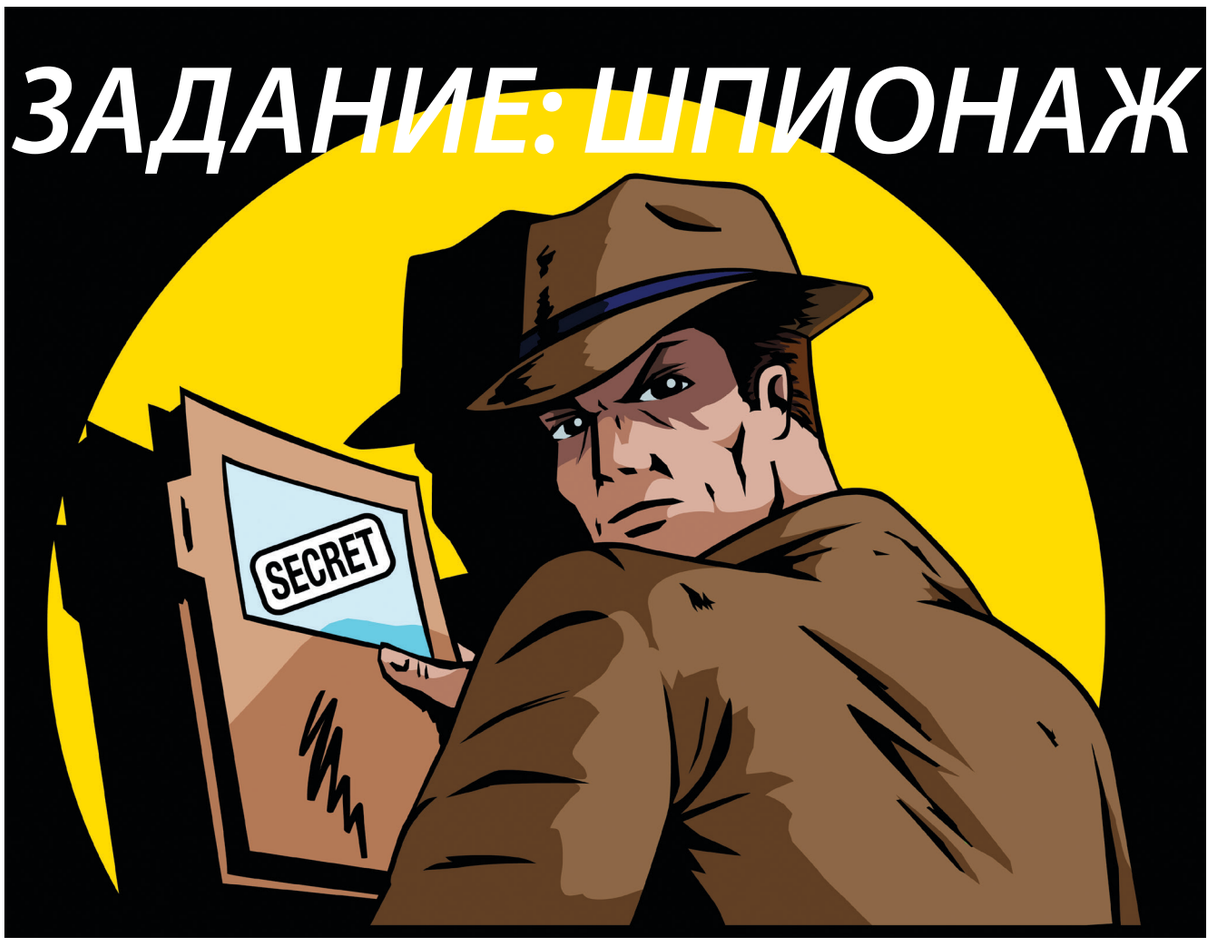
J.I.: Существуют ли риски информационной безопасности при ИБ-аутсорсинге? Назовите наиболее критичные из них.

Ю.Л.: Как и в любом виде деятельности, риски здесь существуют. Основной – кто виноват в случившемся, кто должен платить, если был ущерб, и сколько именно, особенно если это связано с репутационными рисками, отказами в обслуживании и т.п. В данном случае может помочь только грамотно прописанный NDA (Non Disclosure Agreement).

J.I.: На какие критерии следует обращать внимание при выборе партнера?

Ю.Л.: На опыт работы, реализованные проекты, количество и компетенции сотрудников, также нужно учитывать, сколько лет компания существует на рынке, ее годовой оборот, прибыль и т.п. В общем, при выборе аутсорсера необходимо смотреть на все факторы в совокупности, а не только на непосредственный предмет договора. JI

ЗАДАНИЕ: ШПИОНАЖ



Многолетний архив Jet Info содержит статьи, посвященные любым аспектам жизни ИТ-технологий. И многие из них не потеряли своей актуальности, несмотря на прошедшие с момента публикации десятилетия. Сегодня мы решили поднять из архива эссе, автор которого за 3 дня смог завладеть коммерческими секретами крупной корпорации стоимостью в миллиарды долларов. Произошло это в 1996 году (статья была напечатана в Jet Info № 19, 1996), но компании и по сей день сталкиваются с подобными проблемами. Итак, заказным промышленным шпионажем занимается ***Ira S. Winkler, Национальная ассоциация информационной безопасности США.***

ПРЕДИСЛОВИЕ ДЛЯ ЧИТАТЕЛЕЙ JET INFO

В данной статье детально описан процесс кражи коммерческих секретов, стоящих миллиарды долларов. Статья, конечно, задумывалась не как учебник по воровству. Цель ее написания состояла в том, чтобы продемонстрировать важность базовых механизмов безопасности. Почти все упомянутые в статье действия можно предотвратить посредством очень простых контрмер. Например, элементарное наличие политики проверки обоснованности запросов критичной информации, политики, предписывающей связываться с руководителем запрашивающего, позволило бы обнаружить и остановить атаку. Надеюсь, что моя статья послужит своевременным предостережением.

Мне приходилось слышать возражения, что, мол, моя статья все же является учебным пособием по воровству. Думаю, что плохие парни и так знают, как обделывать подобные дела. Типичный пользователь — вот

кто не осознает важности таких элементарных мер безопасности, как защита паролей. Он (пользователь) что-то слышал о промышленном шпионаже и других напастях, но считает, что зло обойдет его компьютер стороной, поэтому продолжает жить так, как жил раньше, то есть безалаберно. На самом деле, пользователи находятся на переднем крае обороны и могут легко остановить даже самые изощренные атаки.

Надеюсь также, что моя статья послужит встряской для профессионалов в области безопасности, которые норовят сосредоточиться на технических деталях типа длины ключа шифрования, игнорируя при этом основы. Помните, что даже лучшие криптографические средства и операционные системы не способны помешать пользователю передать кому-то информацию, к которой он имеет доступ.

УКРАСТЬ ЗА ТРИ ДНЯ

Я положил перед сидевшим молча президентом полную инструкцию по изготовлению самого важного из продуктов, разрабатываемых его компанией. Президент продолжал молчать, когда на его стол лег развернутый план разработок компании. Президент откинулся на спинку кресла, когда к стопке добавились несколько документов, описывающих ход переговоров по поводу состояния многомиллионного судебного процесса. Наконец, президент промолвил: «Мы должны благодарить Бога, что Вы не работаете на наших конкурентов».

Я украл все это и еще кое-что, будучи временным работником. Думаете, речь идет о компании с третьесортной службой безопасности? Едва ли. Внешняя защита организована превосходно, она включает в себя строгий контроль доступа и механизмы физической защиты. Однако руководитель службы безопасности подозревал, что компания может быть уязвима по отношению к хорошо скоординированным атакам с участием штатных работников. Он обратился ко мне, чтобы проверить, что может украсть целенаправленно действующий информационный вор.

На работу в компании мне отвели три дня. Я украл все.

ЗАДАНИЕ

На недавней конференции я встретил Генри, руководителя службы безопасности Zed Technologies (название компании, имена действующих лиц и некоторые технические детали изменены) — большой, высокотехнологичной компании с годовым оборотом более 5 миллиардов долларов. Генри знал о моих предыдущих «контрольных проникновениях» и попросил о последующей встрече с целью обсудить возможность тестирования безопасности его компании.

Генри был крайне озабочен открытостью рабочей обстановки в Zed Technologies — открытостью, типичной для исследовательских компаний. Подобно многим большим компаниям, Zed Technologies использовала труд многих временных служащих и контрактников, предоставляя им рабочие места в своем здании. Эти люди получали доступ к различным объемам информации, не подвергаясь всестороннему контролю. Генри волновал потенциальный ущерб, который эти люди могли нанести компании. Чтобы проверить обоснованность своих опасений, он попросил меня осуществить тестовое проникновение, при котором я буду включен в штат компании как временный работник, но на самом деле попытаюсь украсть как можно больше информации.

Мне разрешили делать все, что я сочту нужным, не нанося при этом вреда компании и людям. Во время моих незаконных действий поблизости все время должен был находиться сотрудник отдела информационной безопасности компании, чтобы уладить инцидент, если меня разоблачат. Я получил также разрешение на привлечение внешних сообщников.

Чтобы промоделировать реальную ситуацию, я решил осуществить полномасштабную попытку промышленного шпионажа против компании, используя как технические, так и нетехнические методы. Более конкретно, я остановился на пяти видах атак:

- поиск по открытым источникам;
- маскарад;
- превышение прав доступа;
- хакерство штатного сотрудника;
- внутренняя координация действий внешних сообщников.

ДАВАЙТЕ ПОЗНАКОМИМСЯ

До встречи с Генри я ничего не знал о Zed Technologies. Мне предстояло в первую очередь познакомиться с компанией, чтобы воровать полезную информацию.

В библиотеках Интернет удалось найти невероятное количество сведений. Из баз новостей я узнал о наиболее успешной разработке компании, стоящей миллиарды долларов, если иметь в виду затраченные усилия и потенциальные продажи. Я узнал также имя ведущего специалиста, работающего над проектом, и прочитал несколько статей о текущих продуктах компании

и о людях, участвовавших в их разработке.

Другие открытые источники позволили узнать имена руководителей компании, ее финансовое положение, а также полу-

чить большое количество общей информации о компании и ее корпоративной философии. Поиск названия компании в группах новостей Интернет выявил десятки ее сотрудников. Письма работников в компьютерные группы новостей рассказали мне об аппаратной и программной среде компании. Письма в прочие группы помогли узнать личные интересы авторов. Другие Интернет-ресурсы позволили выявить некоторых других сотрудников компании и их интересы.

Я запросил сервер имен области сетевого управления Zed Technologies на предмет получения списка всех компьютерных систем вместе с информацией об операционной среде. Данное действие выявило TCP/IP-адреса компании, типы используемых систем и примерное число компьютеров.

Помог и информационный бюллетень компании, который я запросил и получил. В нем президент определил шесть наиболее важных разработок и упомянул имена многих сотрудников, работающих над соответствующими проектами. Имея на руках этот «список покупок», я принялся за выполнение следующих этапов моего плана.

НАГЛАЯ ЛОЖЬ

Поскольку шнырять по компании я мог всего лишь три дня, я вынужден был действовать наглее, чем обычный промышленный шпион. Я попытался осуществить прямолинейный маскарад, решив выдать себя за контролера информационной безопасности.

Прежде чем прибыть на работу, я запасся визитными карточками, которые выглядели точно так же, как карточки сотрудников Zed Technologies. На карточках было напечатано мое имя и должность — Контролер Информационной Безопасности. Их изготовили для меня в местной копировальной лавке меньше чем за день, используя в качестве образца подлинную визитную карточку.

По прибытии в здание компании я был обслужен наравне с другими временными служащими. Я заполнил несколько бланков ложной информацией, скрыв свой номер социального страхования, адрес и телефон. Работник отдела кадров выдал мне идентификационную карточку для прохода и провел на мое рабочее место. Я порадовался, обнаружив, что мое имя было заранее включено в телефонный справочник — таковы принятые в компании правила, действующие по отношению ко всем временным служащим.

Сомневаясь в реакции на мою уловку, я начал шпионскую деятельность с телефонного звонка исследователю, работавшему над важнейшим проектом компании. Я сказал ему, что меня только что приняли в штат и что моя основная задача — защита секретов компании. В этой связи мне необходимо выяснить, что в наибольшей степени нуждается в защите и где хранится соответствующая информация. После обсуждения, длившегося несколько минут, исследователь посоветовал мне обратиться к Стенли — руководителю проекта. Я позвонил Стенли и договорился о встрече с ним.

Играть роль промышленного шпиона было, как говорят в театре, очень волнительно. Меня интересовало, что я буду говорить и делать, если меня поймают. Я почти желал, чтобы кто-нибудь поставил под сомнение мою легенду и мне пришлось бы проверить свою способность выпуты-

ваться. Однако изворачиваться мне не пришлось. Ни один сотрудник не попытался оспорить мою честность.

Встретившись со Стенли, я вновь представился как только что принятый на работу контролер информационной безопасности. Я вручил ему визитную карточку и заявил, что передо мной поставлена задача защиты корпоративной информации. Я попросил объяснить, какая информация является критичной и как много людей имеют доступ к ней.

Стенли объяснил, что в длинном ряду важной информации наиболее критичными являются сведения об изготовлении продуктов. Я поинтересовался, существует ли единый источник этих сведений. В ответ он показал книгу с копиями протоколов заседаний проектной группы и с перечнем лиц, получающих эти протоколы. Я нагло попросил сделать мне копии. Стенли не только передал мне полную копию книги, но и добавил меня в список рассылки протоколов.

Стенли оказал мне еще одну услугу — он рассказал, что представитель правительства в компании и администратор проекта вместе собрали сводную информацию о проекте, и посоветовал поговорить с ними. Я так и сделал. Закончив разговор со Стенли, я вернулся к себе в кабинет и договорился о встрече с Марком — представителем правительства.

С Марком я снова использовал фальшивую визитную карточку и байку про работу в отделе информационной безопасности. Хотите верьте, хотите нет, мне начало надоедать играть роль администратора безопасности, расспрашивающего людей об обработке и хранении критичной информации. Тем не менее я заставлял себя не выходить из образа и вести беседу о массе мелких деталей. Но, как говорится, терпение и труд все перетрут. Мы с Марком подробно обсудили упорядочение документации правительственного представительства, в том числе типы подготавливаемых документов, расположение соответствующих файлов в компьютерной сети компании, работу группы, отвечающей за резервное копирование этих файлов, и имя сотрудника, обеспечивающего сохранность информации. Марк даже упомянул об одном особенно интересном для меня документе, содержащем полную спецификацию процесса производства самого важного продукта компании.

Я вновь вернулся к себе в кабинет и потратил некоторое время на изучение протоколов заседаний исследовательской группы, переданных мне Стенли. Среди изобилия конфиденциальной информации я обнаружил настоящий подарок в виде записки от Марка, правительственного представителя. В этой записке Марк называл место, где расположен проект документа, представляемого американскому правительству. В следующем предложении сообщался пароль, используемый для доступа к документу.

Я не мог поверить своим глазам. Два предложения дали мне ключ к документу, содержащему всю технологическую информацию о проекте, являвшемся моей главной целью. Я сел за компьютер, без проблем добрался до документа и скопировал его. Тем самым я уже украл информации больше чем на миллиард долларов, если учитывать усилия, затраченные компанией, и потенциальные продажи.

Мое изумление еще более возросло, когда в том же каталоге, где я только что нашел подлинный бриллиант, располагались и словно сами просили их украсть аналогичные документы, описывающие еще две важные разработки компании. К этому моменту, менее чем за день, я скомпрометировал три важнейшие разработки Zed Technologies. На основании добытой информации я мог сам начать производство уникальных продуктов.

Воодушевленный успехом, я начал исследовать другие файловые системы, не защищенные паролями. Я пробовал только те каталоги, где, как я надеялся после встреч со Стенли и Марком, могла располагаться критически важная информация. Я не хотел, чтобы ненужные документы дезорганизовали мою работу. За несколько часов я получил более 125 мегабайт данных.

На следующий день я встретился со Стивом, администратором второго по важности проекта компании. К этому моменту все сомнения в успехе моей миссии улетучились. Пришло время заняться информацией, которую создавали и использовали управленцы.

Снова заявив, что мне нужно осмотреть все, за что я отвечаю как член группы информационной безопасности, я попросил Стива воспроизвести процесс доступа к его файлам. Я попытался подсмотреть вводимый им пароль, но с моего места клавиатуры не было видно. Стив подчеркнул важность квартальных управленческих отчетов, которые, по его словам, содержали такую крайне конфиденциальную информацию, как технологические детали. Пока Стив говорил, я заметил, что в двери его кабинета нет замка. Я не мог не заметить также лежавшей на столе коробки с дискетами с надписью «Управленческие отчеты».

Вернувшись в кабинет, я немедленно попытался войти в файловую систему Стива. Я попробовал несколько употребительных паролей и очень развеселился, когда один из них подошел и я получил желаемый доступ. Как оказалось, каждый управленец отвечает за несколько проектов, поэтому в файлах Стива содержались детали многих разработок.

Мое ликование достигло небывалых высот, когда я обнаружил, что все управленцы используют для хранения своих файлов одну файловую систему. Дискеты со стола Стива оказались не нужны. Передо мной лежали управленческие отчеты по всем проектам, значившимся в моем «списке покупок». Я выиграл джекпот.

Позже я узнал, что скомпрометировал все важнейшие разработки компании, кроме одной, а проработал я всего полтора дня. Никто не заметил ничего подозрительного. Никто не сорвал мой покров. Настоящий промышленный шпион улетел бы из города ближайшим рейсом.

ВЕЧЕРНИЕ ПОХОЖДЕНИЯ

Маскарад был только одним из намеченных видов атаки. Как вы, возможно, помните, компания выдала мне идентификационную карточку для прохода. Отработав первый день в Zed Technologies и превосходно поужинав, я вернулся в офис, воспользовавшись моей карточкой.

В здании работали несколько уборщиков, когда я принялся высматривать незапертые кабинеты, шкафы и ящики. Меня интересовали также компьютеры, не защищенные, вопреки требованиям политики безопасности компании, запирающей утилитой. Миновать уборщиков было невозможно, поэтому я решил и не пытаться скрывать свое присутствие. Это было рискованно, но зато уборщики могли сделать вывод, что я не делаю ничего такого, что стоило бы скрывать.

В первой предварительно намеченной мной области, где располагались юридический и лицензионный отделы, я раздобыл документы о продвинутой разработке, включая анализ достоинств и недостатков каждого из потенциальных лицензиатов. Я нашел также хороший материал по отложенным судебным делам, в том числе сведения о переговорах по поводу хода дел. Наконец, моей добычей стал полный, но еще не подшитый текст патента.

Я перешел во вторую из намеченных областей, которую занимали разработчики. Здесь, прямо на столах, мне попались отчеты о проблемах, присущих создаваемым продуктам, и другие конфиденциальные материалы.

В незапертых шкафах я нашел технологическую информацию по двум дополнительным проектам, стоивших сотни миллионов долларов, если считать сделанные инвестиции и потенциальные продажи.

Один из кабинетов, которые я посетил, больше походил на свалку. Бумаги были разбросаны по всей площади, а два компьютера были оставлены без запирающей утилиты. Мониторы были выключены, но я просто включил один из них и увидел, что сотрудник не вышел из программы просмотра почты. К счастью для меня, этот человек предпочитал сохранять электронные письма. Я стал просматривать корреспонденцию, пока не наткнулся на основной график разработок — один из

самых конфиденциальных документов компании.

Шнырянье в нерабочее время может показаться старомодным и примитивным, но эта деятельность позволила мне добыть огромное количество критичной информации. Шпионаж предполагает использование простых, но эффективных методов. В данном случае один вечер работы продемонстрировал выгоду от элементарного поиска незащищенной информации. Я не вскрыл ни один замок и не оставил никаких следов насильственного проникновения.

ХАКЕРСТВО ШТАТНОГО СОТРУДНИКА

Я принес с собой в Zed Technologies переносной компьютер фирмы Sun, специально сконфигурированный для хакерских действий против компании. При конфигурировании я использовал информацию, почерпнутую мной из открытых источников. Я установил на компьютер Интернет-сканер компании Internet Security Systems Inc. и множество хакерских инструментов, помогающих «взламывать» системы, используя бреши, выявленные сканером. Придя в свой кабинет в Zed Technologies, я отключил от сети Ethernet офисный ПК, вместо которого присоединил переносной компьютер Sun.

В первую очередь я «напустил» Интернет-сканер на ключевые компьютерные системы компании, и, как и следовало ожидать, он выявил известные слабости в нескольких экспортируемых файловых системах, которые, как мне было известно, содержали критичную информацию. Затем, после сканирования стандартного набора входных имен, настал черед подбора паролей. Три входных имени были мгновенно скомпрометированы.

Я смонтировал экспортируемые файловые системы на свой компьютер и попытался скопировать себе критичные каталоги. Большую часть мне скопировать удалось, но меня задело, что доступ к части файлов был ограничен. Я вошел в одну из удаленных систем, используя одно из скомпрометированных входных имен, и скопировал туда заготовленную хакерскую программу. Я не особенно надеялся на успех этой акции, но все же запустил программу — вдруг сработает?

Я буквально подскочил на стуле, когда на экране появилось приглашение «#» — я получил права суперпользователя. Теперь единственное, что ограничивало меня, — это емкость дисков моего компьютера. Я скопировал все, что казалось важным. Воспользовавшись еще несколькими потайными ходами, я вошел и в другие системы.

Таким манером мне удалось получить более 200 мегабайт информации, представлявшей чрезвычайную ценность. Слабость, которую я использовал, была выявлена недавно, однако заплата для ее устранения уже была доступна. Компания Zed Technologies немного задержалась с ее установкой. В следующий раз им придется поторопиться.

ХАКЕРСТВО С ДРУЗЬЯМИ

Во время моих маскарадных действий, когда я выдавал себя за сотрудника службы информационной безопасности, я узнал, что в Zed Technologies для аутентификации при удаленном доступе используются интеллектуальные карты. Я раздобыл бланк для заказа таких карт, подделал подпись администратора безопасности и убедил секретаря обойти

все необходимые инстанции. Тем же манером я запросил пейджер. Все это требовалось мне для заключительной атаки, которую я должен был вести во взаимодействии с внешними сообщниками.

Воспользовавшись услугами курьера, я отправил карту и сопутствующее программное обеспечение своим сообщникам, предоставив им тем самым удаленный доступ к Novell'овской сети компании. По телефону я сообщил им свое входное имя и пароль для сети компьютеров Sun, в которую я имел доступ как временный сотрудник. От меня сообщники узнали телефонный номер, обслуживаемый модемом; ранее этот номер сообщил мне один из системных администраторов. Теперь мои бойцы могли скомпрометировать и сеть компьютеров Sun.

Обращение к серверу имен, выполненное мной до начала работы в Zed Technologies, позволило узнать, что в компании используется большое количество Sun-совместимых и PC-совместимых компьютеров. Зная это, я запасся соответствующим хакерским инструментарием и снабдил им своих сообщников. Теперь пришла пора пустить его в ход.

Мои сообщники начали с того, что скачали файл паролей из сети Sun-компьютеров и «напустили» на него программу Crack подбора паролей. Таким образом удалось узнать примерно 10% паролей. Скомпрометированные входные имена и пароли сообщники передали мне по факсу, после чего я упорядочил полученный список по степени важности пользователей, воспользовавшись компьютерным справочником для определения отдела по входному имени сотрудника.

Содержимое ответного факса, направленного мной, составляло упорядоченный список входных имен и ключевые слова, позволяющие выявить критичную информацию. Сообщники произвели поиск в каталогах важнейших пользователей и проникли в некоторые другие компьютерные системы компании, которые выбрали по своему усмотрению. Средства удаленного доступа по коммутируемым линиям, спроектированные для защиты от НСД, не могли остановить авторизованных пользователей.

Один из сообщников сосредоточился на компрометации PC-систем. Используя интеллектуальную карту, он получил доступ по телефонным линиям к внутренней сети. Затем он запустил программу выявления слабостей в нескольких зонах, которые я определил как наиболее ценные. Из атакуемых областей он скопировал большое количество информации.

Координация действий штатным сотрудником стала ключом к успеху нашей деятельности. Даже если обычный внешний злоумышленник сможет преодолеть первую линию обороны (что маловероятно), он не сможет узнать, где искать критичную информацию. Компьютеры компании хранят более терабайта данных, из которых только гигабайт можно считать конфиденциальным. Возможно, размер подлинно критичной информации с технологическими деталями производственных процессов не превышает мегабайта. Сам по себе компьютерный доступ мало что значит; важен доступ к конкретной информации.

НЕКОТОРЫЕ ВЫВОДЫ

По прошествии трех дней, как и планировалось, я оставил вре-

менную работу в Zed Technologies. Я добыл более 300 мегабайт конфиденциальных данных. У меня в руках была детальная информация о технологии производства пяти наиболее важных продуктов компании с суммой потенциальных продаж в миллиарды долларов. Кроме того, я получил большое количество информации практически обо всех новых разработках. Попади она к конкурентам, доходы компании могли резко сократиться. Судя по объему добытой мной информации, весьма вероятно, что у меня в руках оказалась технология производства большинства продуктов компании, но с уверенностью заявить об этом можно было только после тщательного изучения наворованного.

Пока я действовал, никто не заметил ничего подозрительного. Несмотря на мои грубые методы, никто не обратил внимания на то, как я компрометирую важнейшие разработки компании.

Важно отметить, что я ни в коей мере не исчерпал арсенал настоящих промышленных шпионов. Мне это было попросту не нужно. Я не пытался устанавливать «жучки» или прослушивать телефонные линии. Я не вербовал других сотрудников и не копался в мусорных корзинах. Я потратил очень мало времени и денег; планирование и осуществление реальной атаки заняло бы несколько месяцев, а в «дело» вложили бы миллионы долларов.

Многие читатели могут подумать, что Zed Technologies — это компания разгильдяев, безопасность в которой находится на низком уровне. На самом деле, скорее верно обратное. Тот факт, что руководство решило провести описанный тест, доказывает заботу компании о надежной защите критичной информации. К сожалению, в Zed Technologies уделяли внимание только внешнему рубежу обороны. Как только злоумышленник становится штатным работником, внешняя защита перестает действовать, а корпоративная информация подвергается очень серьезному риску.

ОБ АВТОРЕ

На момент выхода статьи ее автор Айрэ Винклер (Ira Winkler) работал в Национальной ассоциации информационной безопасности (National Computer Security Association, NCSA) США (Карлайл, Пенсильвания) в должности директора по технологиям. На этом посту он отвечал за широкий круг вопросов, включая тестирование и сертификацию межсетевых экранов (firewalls), тестовые проникновения, информационные учебные курсы, архитектуру систем безопасности. Он оказал множество разнообразных услуг некоторым крупнейшим в мире компаниям. Он является специалистом в таких областях, как тестовые проникновения, информационное оружие и промышленный шпионаж. Он делал доклады на многих международных конференциях.

Кроме того, мистер Айрэ Винклер обладает сертификатом профессионала в области безопасности информационных систем (Certified Information Systems Security Professional). JI

ЕВГЕНИЙ АКИМОВ,
заместитель директора Центра информационной безопасности компании «Инфосистемы Джет»

17 лет назад в момент выхода этой статьи подобные случаи кражи конфиденциальной информации были единичными и, скорее, заказной демонстрацией наличия самой такой возможности. Мало кто терял деньги или репутацию. Но сегодня ситуация такова, что подобное превратилось в преступный бизнес, в котором злоумышленники зарабатывают, а их жертвы ощутимо теряют. Этот «хакерский конвейер» сократил время от появления той или иной методики взлома до ее «промышленного» использования буквально до считанных дней и даже часов.

Конечно, технические методики, о которых говорится в статье, за прошедшее время стали сложнее и изощреннее. С организационной точки зрения ситуация осталась практически такой же. Как и в 1996 году, происходящие сегодня инциденты ИБ показывают, что именно внутренние пользователи (сотрудники, аутсорсеры, а иногда и аудиторы) осуществляют самые масштабные и болезненные атаки на ИТ-системы. Поэтому вопросы защиты от внутренних злоумышленников – с помощью систем централизованного управления правами доступа (IdM), контроля утечек (DLP), многофакторной аутентификации, контроля действий привилегированных пользователей и администраторов и т.п. – рассматриваются и будут рассматриваться многими компаниями как крайне актуальные и животрепещущие.

Среди отечественных компаний растет заинтересованность в получении услуг ИБ из облака

АВТОР: АЛЕКСЕЙ КОСИХИН

Об основных источниках угроз АСУ ТП, этапах построения эффективной системы защиты АСУ ТП с учетом специфики отечественного бизнеса, услугах ИБ-аутсорсинга и востребованности получения услуг ИБ из облака рассказывает Алексей Косихин, руководитель направления по работе с ТЭК компании «Инфосистемы Джет».

Источник: Connect! Мир связи, № 3, март 2013 г.

Аутсорсинг информационной безопасности – «за» и «против»

АВТОР: АЛЕКСЕЙ ЛАВРУХИН

По мнению директора по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет» Алексея Лаврухина, «на рынке России и стран СНГ активно набирает обороты аутсорсинг в сфере ИТ. Что касается аутсорсинга информационной безопасности, то рынок подобных услуг только формируется». В своей статье Алексей более подробно рассматривает специфику аутсорсинга ИБ, возможные варианты оказания данного сервиса и дает прогнозы на будущее рынка ИБ-аутсорсинга.

Источник: Connect! Мир связи, № 11, ноябрь 2012 г.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Главный редактор: Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01 факс (495) 411 76 02
e-mail: JetInfo@jet.msk.su *http://www.jetinfo.ru*

Подписной индекс по каталогу Роспечати **32555**