ГРУППА КОМПАНИЙ INFOWATCH

Всеволод Вячеславович Иванов
ИСПОЛНИТЕЛЬНЫЙ ДИРЕКТОР

ЭВОЛЮЦИЯ РОЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

Использование информационных технологий сегодня является неотъемлемой частью и необходимым условием работы организации любого типа, от небольшой коммерческой компании до крупного государственного предприятия. Однако с широким распространением информационных технологий возникли новые возможности для злоумышленников, организации оказались лицом к лицу с новыми угрозами. Тогда возникло и начало активно развиваться направление информационной безопасности.

Первым этапом развития стала эра защиты информационных потоков (1990–2005 годы), когда основной задачей информационных технологий было ускорение обмена информацией между организациями. Именно в этот период в Россию с запада пришли первые вирусы, направленные на заражение информационных систем и прерывание процессов обмена информацией. Тогда же появились первые российские хакеры (исследователи вирусов, программ и операционных систем) и первые отечественные антивирусные компании.

Примерно к 2005 году, помимо вирусной активности, в области информационной безопасности (ИБ) назрела другая проблема: стало очевидно, что конфиденциальные данные, хранящиеся в информационных системах предприятий, подвержены утечкам. Эти данные похищают, повреждают и уничтожают как внешние злоумышленники (хакеры), так и внутренние (нелояльные, обиженные или просто подкупленные конкурентами сотрудники компаний). И с этой проблемой надо было как-то бороться. Так наступила эра защиты данных (2005–2012 годы), когда основной задачей ИБ стало обеспечение безопасного хранения и передачи данных. В эти годы возникло и выделилось в отдельный сегмент направление по защите данных от утечки – DLP (Data Leak Prevention). Пионером и лидером отечественного DLP-рынка стала компания InfoWatch.

К 2012 году информационные технологии эволюционировали настолько, что сделали большинство сервисов доступными онлайн. По сути, информационные технологии превратились в полноценную бизнес-среду, позволяющую совершать электронные платежи, пользоваться онлайн-банкингом, осуществлять электронное принятие решений, проводить виртуальные совещания, работать удаленно с помощью мобильных устройств. В этом процессе роль ИБ изменилась: из чисто технической сфера ИБ превратилась в важный инструмент защиты бизнеса, обеспечивающий успешное функционирование бизнес-процессов и развитие компании в целом. Этот период, в котором мы с вами сейчас живем, можно назвать эрой защиты бизнеса.

ВНУТРЕННИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Основанная как DLP-вендор, сегодня группа компаний InfoWatch объединяет несколько организаций, которые разрабатывают комплексные решения в области ИБ, защиты корпоративной информации на основе собственных технологий лингвистического анализа, а также инструменты для управления бизнес-рисками: InfoWatch, KRIBRUM, EgoSecure, APPERCUT, Cezurity, Taiga.

Группа компаний InfoWatch предлагает решения для защиты бизнеса от всех видов угроз ИБ, как внутренних, так и внешних. Разделение угроз на внутренние и внешние подразумевает различный источник: внутренние угрозы исходят от сотрудников, внешние – от хакеров и прочих злоумышленников, не принадлежащих к организации.

Самые распространенные внутренние угрозы – это кража корпоративной информации сотрудниками или ее утечка по неосторожности, а также действия нелояльных сотрудников против компании: мошенничество, саботаж и даже банальное разгильдяйство.

Любопытную закономерность можно заметить, проанализировав статистику внутренних угроз ИБ за последние несколько лет. Если в 2012 году из 214 внутренних инцидентов, выявленных InfoWatch, 81% был связан непосредственно с утечкой данных и лишь 19% – с прочими внутренними угрозами, то уже в 2014 году наблюдалась ровно противоположная ситуация: из 331 проанализированного нами инцидента менее половины (41%) представляли собой утечку информации. В остальных 59% случаев система зафиксировала попытки саботажа, коррупционной деятельности или мошенничества. Это означает, что сегодня компании несут значительные потери уже не столько от кражи данных, сколько от действий нелояльных сотрудников. Таким образом, защита предприятий от внутренних угроз является не только областью информационной, но и в первую очередь экономической безопасности компаний.

Следует отметить, что сейчас вносит свои коррективы и кризис. По наблюдениям

руководителей по ИБ российских компаний, число инцидентов, связанных с хищениями информации, по сравнению с докризисным периодом возросло в три раза.

Так, аналитический центр InfoWatch недавно провел опрос среди клиентов InfoWatch в России, задав им вопрос: «Хотите ли вы сократить затраты на ИБ в кризис?». Результаты показали, что 44% компаний планируют увеличить свои расходы на ИБ и еще 35% – оставить затраты на том же уровне. Это значит, что подавляющее большинство компаний не планирует экономить на ИБ, и это более чем разумная стратегия.

Для защиты от внутренних угроз InfoWatch предлагает решение InfoWatch Traffic Monitor, много лет подряд удерживающее лидерство в данном сегменте. Данная система анализирует всю информацию, обращающуюся в компании, и выявляет нелегитимную передачу конфиденциальных данных. Решение позволяет выявлять и предотвращать утечки информации по всем ключевым каналам: через корпоративную и электронную почту, Skype и другие мессенджеры, при записи на съемные носители или выводе на печать и т.д.

Уникальные лингвистические технологии InfoWatch позволяют распознавать документы и понимать их смысл даже при анализе небольших фрагментов текста, которые могут быть вставлены в любой документ или отправлены сотрудником компании вовне в неформальной переписке.

Благодаря встроенным инструментам взаимодействия с HR-службой, InfoWatch Traffic Monitor учитывает больше данных для формирования картины угроз, чем традиционные DLP-системы. Продукт позволяет настраивать и применять особые целевые политики контроля персонала, входящего в так называемую группу риска, с созданием специальных отчетов об активности подобных сотрудников и применением к ним более строгих политик безопасности. К группе риска традиционно относят сотрудников, планирующих увольняться или находящихся на испытательном сроке, ведь именно по их вине происходит большинство утечек информации.

InfoWatch Traffic Monitor на ранней стадии выявляет сговоры, мошеннические и коррупционные действия сотрудников. Вся информация об инцидентах, связанных с персоналом, хранится таким образом, чтобы ее при необходимости можно было использовать в качестве доказательной базы против нарушителя в суде.

Курс на развитие продукта в сторону защиты от полного спектра внутренних угроз, а не только от утечек был взят компанией InfoWatch 3 года назад. В результате сегодня компания демонстрирует не только безусловное лидерство на рынке, но и самый быстрый рост среди конкурентов.

Кроме того, InfoWatch уделяет много внимания качеству обслуживания клиентов. Во-первых, процедура внедрения, разработанная компанией, подразумевает совместное с клиентом построение модели угроз информационной безопасности, на время внедрения каждой компании-клиенту предоставляется персональный аналитик и лингвист, задача которых – провести качественную категоризацию всей информации в компании.

Неотъемлемой частью процесса внедрения решений InfoWatch является разработанный экспертами InfoWatch Pre-DLP Toolkit. Это комплект из 26 документов, предоставляемый заказчику на первоначальном этапе, благодаря чему становится возможным юридически и процедурно грамотно внедрить InfoWatch Traffic Monitor. Кроме того, пакет документов Pre-DLP включает практические рекомендации по защите корпоративных данных от утечек, разработанные специалистами InfoWatch на основе 10-летнего опыта внедрения DLP-систем на российских предприятиях различных отраслей экономики.

Необходимость в столь детализированном подходе продиктована тем, что только грамотный консалтинг на этапе внедрения решения обеспечивает эффективность работы системы. От правильно проведенного внедрения в дальнейшем зависит и успешность расследования инцидентов ИБ, выявление нарушителей и привлечение их к ответственности.

Часть компаний используют DLP-системы для мониторинга, а не блокировки утечек информации. В этом случае абсолютно необходимым инструментом для заказчика является разработанный специалистами InfoWatch Post-DLP Toolkit. Он включает в себя 13 документов с рекомендациями по процедуре корректного расследования инцидентов, связанных с внутренними угрозами ИБ компаний, сбора юридически значимой доказательной базы для рассмотрения дел о нарушении конфиденциальности информации в суде.

В частности, в Post-DLP Toolkit входят рекомендации по увольнению за разглашение и процедуре увольнения; чек-лист «Сбор информации об инциденте»; шаблоны документов, необходимых для увольнения работников за разглашение охраняемой законом тайны (докладной записки, приказа о создании комиссии, уведомления о необходимости письменных объяснений, акта об отказе давать объяснения, приказа о прекращении трудового договора и др.).

Всё это позволяет организациям любого размера быстро и без собственных ресурсозатрат внедрять решение для комплексной защиты от внутренних угроз.

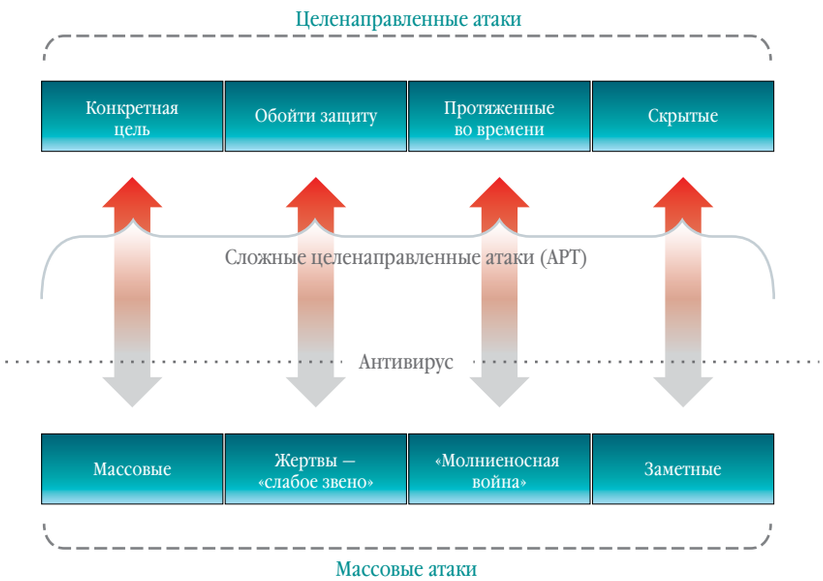
Другая угроза со стороны сотрудников – распространение конфиденциальной информации или негатива в отношении компании в социальных медиа, таких как Facebook, Twitter, «ВКонтакте», «Одноклассники» и др. Такие действия трудно отследить, если они осуществляются с домашнего компьютера сотрудника. При этом они могут нанести серьезный ущерб репутации компании и вызвать отток клиентов. Для выявления таких публикаций ГК InfoWatch предлагает решение InfoWatch KRIBRUM. Данная система представляет собой облачный сервис мониторинга социальных медиа – обсуждений брендов, компаний или персон в Интернете.

В случае если организация прибегает к услугам по написанию заказного программного кода, она сталкивается с еще одной угрозой – что программисты оставят «закладку» в коде. Поскольку редкое тиражное бизнес-приложение целиком удовлетворяет требованиям организации, 90% крупных и средних компаний дорабатывают их своими силами (ERP, АБС, CRM), а значит, есть риск, что в ПО будут реализованы недокументированные возможности. При этом анализ кода бизнес-приложений на наличие «закладок» чаще всего проводится вручную или никак, поскольку во многих системах используются собственные языки программирования и для выявления случайных или умышленных «закладок» нужно быть экспертом в программировании на этом языке.

Большинство «закладок» внедряется программистами не для противоправных действий, а для отладочных работ и оперативного внесения изменений в бизнес-приложение в обход бюрократических процедур. Но программист волен наделить «закладку» в бизнес-приложении любыми возможностями. Для защиты от этих рисков было разработано решение InfoWatch APPERCUT – система анализа кода бизнес-приложений для защиты от «закладок» и недокументированных возможностей.

НА СТРАЖЕ КИБЕРГРАНИЦ

Таргетированные атаки впервые стали предметом активных дискуссий мирового сообщества еще в 2009 году. Тогда стало известно об атаке Stuxnet. Пожалуй, можно сказать, что с нее и началась новейшая история целенаправленных кибератак. Таргетированные (или целенаправленные) атаки – это заранее спланированные действия против конкретной государственной или негосударственной структуры либо организации.



1. РАЗЛИЧИЯ МЕЖДУ ЦЕЛЕНАПРАВЛЕННЫМИ И МАССОВЫМИ АТАКАМИ

2. СТРУКТУРА ДАННЫХ, НАИБОЛЕЕ ЧАСТО ПОХИЩАЕМЫХ ПРИ ПОМОЩИ ЦЕЛЕНАПРАВЛЕННЫХ АТАК

При этом атакующая сторона пытается адаптироваться под собственную инфраструктуру компании и сделать атаку максимально незаметной. Она должна быть либо обнаружена как можно позже, либо не обнаружена вообще. Поэтому подобные атаки, как правило, протяженны во времени и становятся заметны только тогда, когда приходит время активно проявить себя.

На сегодняшний день существует несколько основных методов выявления целенаправленных атак на ранней стадии. Первый – это сигнатурный анализ, являющийся основой антивирусных решений. Однако минус этого подхода состоит в том, что для успешного распознавания вируса его сигнатура должна быть занесена в базу. Но, поскольку для целенаправленных атак хакеры разрабатывают уникальное ПО, которого нет в сигнатурных базах, сигнатурный анализ оказывается бесполезным.

Другой метод изучения уже выявленного ранее вредоносного ПО – это эвристический анализ. Его основная функция заключается в том, чтобы проверять исполняемый код на наличие подозрительной активности, характерной для деятельности вирусов. Подобная методика хороша тем, что не зависит от каких-либо баз. Однако и у эвристического анализа есть свои минусы. Ввиду того что все основные антивирусы известны и доступны для использования всем желающим, хакеры могут производить тестирование написанного ПО и видоизменять его до тех пор, пока оно не будет обходить все известные средства антивирусной защиты. Тем самым эффективность основных эвристических алгоритмов сводится на нет.

Еще один популярный подход – тестирование программ в «песочнице», то есть на имитаторе информационной системы предприятия. Весь трафик перенаправляется в такую «песочницу», после чего производится наблюдение за действиями ПО. К сожалению, и этот метод часто не оправдывает себя, поскольку злоумышленники научились обходить эту защиту. Сейчас всё чаще встречаются вирусы, распознающие, находятся ли они в «песочнице» или в реальной информационной системе. В первом случае такие решения никак не демонстрируют вредоносную функциональность и только спустя время проявляют свои возможности.

В 2014 году InfoWatch предложила принципиально новый подход к решению проблемы, реализованный в продуктах для выявления целенаправленных атак InfoWatch Targeted Attack Detector и InfoWatch Targeted Attack Monitor. Использованная в них технология динамического обнаружения аномалий в информационной системе не имеет аналогов в мире. Программа осуществляет регулярное динамическое сканирование информационной системы организации на наличие аномальных изменений. Если такие аномалии выявлены, система защиты отправляет данные о них в специализированное облако, в котором производится их анализ и оценка.

Решения InfoWatch распознают любую аномалию в системе, в том числе вредоносное ПО, ведущее себя дружественно в эмулированной среде. Система проста во внедрении и использовании, ее преимущества были по достоинству оценены заказчиками. Это продуктовое предложение принесло InfoWatch несколько новых клиентов и первую прибыль по данному направлению в конце 2014 года.

В завершение хотелось бы еще раз отметить, что ИБ, как и информационные технологии, оказывает всё большее влияние на деятельность любых компаний. Поэтому только организации, которые уделяют безопасности достаточно внимания и подходят к защите информации комплексно, смогут защитить свой бизнес и продолжать двигаться в ногу со временем.

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

ЗАО «ИНФОВОТЧ»

2-Я ЗВЕНИГОРОДСКАЯ УЛ., Д. 13, СТР. 41,
МОСКВА, РОССИЯ, 123022
ТЕЛ./ФАКС: (495) 229 0022
E-MAIL: INFO@INFOWATCH.RU
WEB: WWW.INFOWATCH.RU