14 сентября 2017

# Не единым антивирусом: что нужно знать о защите информационных активов бизнеса

О главных мифах в области информационной безопасности из-за которых компании теряют деньги и о способах их предотвращения рассказывает Анатолий Маковецкий, ведущий инженер по информационной безопасности департамента ИТ-аутсорсинга ГК «КОРУС Консалтинг».
Каждый день в мире совершается 117 339 кибератак. Показатель подтвержденных финансовых убытков, связанных с инцидентами в сфере кибербезопасности в 2016 году по разным оценкам составляет от 1 до 500 млрд долларов США. При этом, согласно исследованию EY по информационной безопасности, в 69% российских компаний именно сотрудников считают основным источником киберугрозы, и только второе место отводят внешним воздействиям.

Широко распространен миф, что кибератакам подвержен только определенный круг организаций — индустрии ИТ и финансов. Несмотря на то, что в эпицентре кибератак действительно традиционно находятся они, начиная с 2013 года кибератаки начали постоянно происходить на компании практически во всех секторах экономики, особенно там, где этого ожидают меньше всего. Поэтому такие компании максимально уязвимы. Так, по

данным Deloitte, под особой угрозой следующие отрасли:

**Онлайн-медиа.** Веб-сервисы — основная мишень преступников. Хакеры могут несанкционированно опубликовать информацию не соответствующую действительности, либо порочащую чью-то репутацию или вывести сервис из строя. Все это ведет к потере доверия читателей, их возможному оттоку и длительным судебным тяжбам.

**Телекоммуникации.** Отрасль, где ИТ-инфраструктура чрезвычайно важна, поскольку обеспечивает передачу данных клиентов, а также обрабатывает и хранит большие объемы пользовательских данных. Злоумышленники могут вывести из строя часть инфраструктуры или украсть данные клиентов. Это грозит финансовыми потерями за простой, компенсациями потерь клиентов, судебными издержками и потерей репутации.

**Электронная коммерция.** Через публичные сервисы можно добраться до инфраструктуры владельца ресурсов и украсть важные данные. Главная опасность для компаний — многомиллионные издержки на возмещение потерянных клиентами данных и денег с карт, отток клиентов и репутационные потери.

**Промышленность.** Кроме кибершпионажа и кражи ценной информации об организации процессов, которые давали конкурентное преимущество, преступник может полностью остановить процесс производства. Так, например, было при недавней атаке вируса WannaCry на информационные системы компании Renault, которая понесла колоссальные убытки при простое производства.

**Розничная торговля.** Часто целью преступников становятся POS-терминалы, заразив которые можно получить данные о банковских картах клиентов, другой вектор атаки — система управления складом и товарами, уничтожение баз данных которой может остановить работу магазинов на неопределенное время и привести к оттоку покупателей.

Последствия крупных атак дорого обходятся любому бизнесу, как с точки зрения моментальных финансовых потерь, так и репутации компании, снижения доверия клиентов, партнеров и государства, то есть потерь в среднесрочной и долгосрочной перспективе. В статье я расскажу о базовых инструментах и процессах, с которых нужно начинать информационную безопасность бизнеса.

## Что сделать в первую очередь

**Понять, кто ваш злоумышленник.** Начинать нужно с «бумажной безопасности» — отдел информационной безопасности или ИТ должны проанализировать инфраструктуру, и подготовить пакет документов, которые будут закладывать основу для безопасности. Один из основных документов — это «Модель угроз», именно в нем указываются все возможные угрозы для компании, которые могут прямо и косвенно привести к финансовым потерям. Реализация угроз может нанести репутационный ущерб, временную потерю работоспособности инфраструктуры, утерю доверия стейкхолдеров, прямые финансовые издержки. Также необходимо в общем виде определить возможные методы борьбы, начиная с простых, как установка паролей на базовую систему ввода-вывода компьютеров — BIOS и контроля целостности технических средств и помещений — заканчивая сложными облачными

аналитическими системами для поиска подозрительной активности. Следующим шагом может стать формирование «Модели нарушителя» — документа, в котором описывается квалификация преступника, который мог бы реализовать ту или иную угрозу.

**Приоритезировать.** Представьте, что вы уезжаете в отпуск и хотите сохранить имущество в целостности. Если злоумышленник попробует сломать стену, подкопать и разобрать пол или разобрать крышу, с большой долей вероятности он привлечет внимание соседей, которые вызовут полицию — разумнее залезть через окно или дверь. Поэтому самым слабым звеном в доме окажется окно или дверь. Так и в информационной безопасности, защищенность всей инфраструктуры равняется защищенности самого слабого ее сегмента.

## Внутренний нарушитель

**Внутренний злоумышленник** — это инсайдер, бывший или нынешний сотрудник организации, а в некоторых случаях — подрядчик или дочерняя компания.

Самая распространенная ситуация, при которой эта группа может способствовать преступлению — простая ошибка. К примеру, человек случайно выложили на публичный портал закрытую документацию или отправил важный файл через социальную сеть, не ограничив к нему доступ. Люди всегда ищут самые простые способы работы и не задумываются о последствиях своих действий. Поэтому в зоне риска все сотрудники, которые имеют доступ к ценной информации, и не обязательно они должны

стремиться навредить.

Второй вариант внутреннего преступления, когда внешний злоумышленник через шантаж или подкуп сотрудника получает доступ к инфраструктуре или ценной информации. Злоумышленником может быть недобропорядочный конкурент, «Робин Гуд» — борец за справедливость, взламывающий коммерческие компании ради идеи, или стажер в отделе логистики увлекающийся ИТ, которому просто важно самоутвердиться.

Последняя категория злоумышленников — обиженные сотрудники или партнеры. Они могли получить отказ в повышении заработной платы или изменении условий сотрудничества и хотят отомстить или доказать что-то обидчику.

## Внешние злоумышленники

Внешнего злоумышленника выявить тяжелее, чем внутреннего — формирование обиды легко проследить, а от внешних преступников можно ждать чего угодно в любой момент. Системы для предотвращения внешних угроз устроены сложнее, они дороже, требуют более четкой организации внутренних процессов, а также содержат более сложные алгоритмы выявления связей и реализации различных угроз.

## Стратегия предотвращения атак и поиска преступников

Простым внедрением системы или средств защиты информации обойтись не получится. Действовать всегда нужно комплексно.

**Люди и регламенты.** Все, что касается доступа к закрытой информации и сервисам нужно обязательно регулировать. Внутренние нарушители опаснее, чем внешние. Поэтому я сторонник строгого подхода в области корпоративной культуры и внутренних правил.

Чтобы точно обезопасить системы, отделу по информационной безопасности стоит наладить тесное взаимодействие с HR-подразделением и получать от них информацию о подозрительных заявлениях, видимых обидах сотрудников и любой другой информации, которая может стать поводом для проблем.

Всю документацию и регламенты, которые касаются взаимодействия сотрудников друг с другом, с корпоративными системами и с прочими лицами, важно привести к понятной и четкой структуре.

Внутренние документы должны регулировать большинство вопросов, возникающих при работе с защищаемой информацией, чтобы пользователи не могли по ошибке поставить информационные активы под угрозу. И только после определения порядка работы с информацией можно задумываться о внедрении специализированных средств для контроля за установленным порядком.

**Инфраструктура**. Использование специализированных решений в сфере информационной безопасности предполагает, что ИТ-инфраструктура компании достаточно зрелая и стабильная, иначе эффект от их использования окажется значительно ниже ожиданий.

**Контроль**. Инфраструктура компании должна находиться под постоянным контролем. Нужно исключить или минимизировать использование неконтролируемых технических средств, к примеру, личных компьютеров и смартфонов при работе с защищаемой информацией. Это важно для того, чтобы в любой момент у руководства компании и отдела ИБ был контроль над всеми коммуникациями в организации и над всеми техническими средствами. Важно также организовать единую точку входа в информационную систему компании для всех сотрудников — в таком случае, выявить отклонения до совершения преступления или найти преступника постфактум можно будет в кратчайшие сроки.

**Физическая безопасность.** Следующая задача — обезопасить данные физически. Если ваш сервер стоит в кладовке рядом с зимней резиной начальника, ведрами уборщицы и вентилятором, это уже опасность. Даже крупные компании часто не уделяют должного внимания физической безопасности технических средств. Я лично был свидетелем, как в одной уважаемой фирме серверная была организована в хозяйственном помещении, доступ в которую был у всех желающих. При неконтролируемом доступе к контроллеру домена за 10 минут можно получить наивысшие привилегии в домене. Чтобы избежать такого простого взлома, физические серверы рекомендуется пломбировать и непрерывно мониторить их доступность — многие сценарии взлома приводят к временной остановке атакуемого сервиса.

**Хранение данных.** Хранить служебную информацию о работе оборудования, сервисов и систем только на самом оборудовании крайне небезопасно. Чтобы обеспечить возможность расследований компании необходимо

отправлять данные вовне — устанавливать дополнительные серверы в разных локациях и копировать информацию в каждого из них, чтобы действия злоумышленников не остались незамеченными.

**Юридическая значимость информации.** Крайне важно, чтобы все накопленные данные могли быть использованы при решении споров, для этого они должны накапливаться на законных основаниях и храниться совместно с метками времени, к которым они относятся. Нужно рассказать о новых правилах сотрудникам, донести, что новая система обеспечения информационной безопасности организации — это не карательный инструмент, а механизм, позволяющий всем быть чистыми и честными друг перед другом, позволяющий избежать ответственности за чужие неправомерные действия. Только в таком случае компания может использовать собранные данные в суде и не встречать противодействие и недовольство со стороны работников. Кроме того, рекомендуется обеспечивать неизменность содержимого журналов и меток времени с помощью средств криптографической защиты информации.

Когда инфраструктура приведена в порядок, физически защищена, а все коммуникации проходят через контролируемые шлюзы, стоит задуматься об использовании специализированных систем и средств защиты информации, которые позволят совершенствовать систему защиты информации предприятия и приблизить максимально ее к концепции, положенной в ее основу.

## Специализированные решения

**DLP.** По определенно настроенным правилам и шаблонам они определяют, что информация предназначена для служебного пользования, выявляют утечки и попытки их совершения, фиксируют, что важная информация выходит за защищаемый периметр. К примеру, DLP-система позволит определить, если кто-то из сотрудников попытается распечатать, отправить по почте или скопировать на внешний накопитель файлы, содержащие информацию ограниченного доступа, либо позволит найти нелояльных сотрудников, которые ищут новые места работы со своих рабочих компьютеров.

**SIEM.** SIEM системы собирают и анализируют информацию из разных источников о событиях ИБ. Как правило, поток информации в организации большой, и любой человек или даже отдел не сможет оперативно отреагировать на аномалии. Современные SIEM-системы позволяют анализировать события, категорировать их и обрабатывать различными способами, в зависимости от их критичности, после чего автоматически осуществлять уведомление ответственных лиц и выполнение запрограммированных действия для качественного реагирования на них.

**MDM (EMM).** MDM и EMM решения позволяют управлять мобильными устройствами, которые обычно организация не может контролировать. К примеру, блокируя конкретные приложения. Использование MDM решений совместно с DLP могут минимизировать или даже нейтрализовать возможность нарушения безопасности информации, обрабатывающейся на контролируемых устройствах. К примеру, MDM-системы могут использоваться для защиты складских терминалов, либо корпоративных мобильных устройств пользователей. Также возможно применения данного

класса решений в концепции BYOD, позволяя защитить корпоративные данные, но не налагая ограничений и не контролируя личные данные пользователей.

**Аналитические системы класса BI и Machine Learning.** Такие решения универсальны, поэтому часто используются при построении систем информационной безопасности, чтобы анализировать информацию, выявлять отклонения, тренды и прогнозировать атаки. Зачастую, некоторые возможности BI и ML закладываются в SIEM-решения. Также аналитические системы могут применяться в комплексных решениях, осуществляющих поведенческий анализ оборудования, пользователей и систем, для выявления новых векторов атак и ранее неизвестных уязвимостей.

**Системы управления корпоративными документами.** К данной категории решений относятся ECM-системы, позволяющие хранить и управлять доступом к документам, а также системы, осуществляющие криптографическую защиту корпоративных документов, их категоризацию и управления доступом, как Microsoft RMS.

**Системы управления уязвимостями** — решения, которые отслеживают появление информации о новых уязвимостях и анализируют контролируемое оборудование на их наличие, в случае выявления уязвимостей, позволяют закрыть их, либо временно решить проблему обходными решениями.

Этот список не исчерпывающий. Очевидно, что внедрение всех подобных инструментов обойдется недешево, да и не всегда такое внедрение будет обосновано. Главное — никогда не забывать об одном из важнейших постулатов построения систем защиты информации — стоимость защиты не

должны превышать стоимость возможного ущерба от реализации угроз безопасности информации.

## Когда начинать задумываться об информационной безопасности?

**Повышение расходов.** Это первый индикатор, что что-то идет не так. Если раньше на определенный процесс требовалось три часа работы, а сейчас, к примеру, пятнадцать часов, это явный признак, что рабочее время расходуется неэффективно, а причина неэффективного использования может оказаться потенциальной угрозой информационной безопасности.

**Резкое падение доходов** в рамках не изменяющейся рыночной ситуации — тоже является важным индикатором нарушения установленных процессов.

**«Сливы» в прессе**. Если резко начали появляться статьи, о внутренних делах компании или о подходах к ведению бизнеса, и они в достаточной мере соответствуют правде, велик шанс, что кто-то из сотрудников «сливает» информацию.

Об информационной безопасности, как и о физической, задумываются поздно — когда кризис близко или уже грянул, и с помощью профилактики проблемы уже не решить. Поэтому к минимизации рисков важно подходить стратегически — это всегда комплекс из управленческих решений и информационных систем, который не ограничивается исключительно антивирусом. При этом начинать разработку стратегии всегда нужно не с систем, а с процессов и регламентов, потому что кроме внешних угроз есть и внутренние — неосторожность, необдуманность, а иногда и умысел

нынешних или бывших сотрудников и партнеров. Если вам есть, что терять, то стоит обратиться как минимум за консультацией к опытным специалистам, которые обнаружат уязвимости и подскажут, какими средствами с ними можно справиться, не раздув бюджет.

*Материал опубликован на портале Global CIO, сентябрь 2017*