Внутренние и внешние ИБ-угрозы: есть ли смысл в их разделении?

ВАЛЕРИЙ ВАСИЛЬЕВ

Усложнение корпоративных ИКТ-инфраструктур и ландшафта киберугроз требует комплексного подхода к организации корпоративной информационной безопасности. Тем не менее по-прежнему принято различать внутренние и внешние ИБ-угрозы и связанные с ними риски. В данном обзоре мы постарались выяснить актуальность разделения ИБ-угроз на внешние и внутренние, определить, где проходит граница между этими видами ИБ-угроз, какие специальные технологии и инструменты используются для противодействия им, в каких структурных компонентах корпоративной ИБ-системы организуется комплексное противодействие обоим видам угроз.

ОБЗОР

Актуальность разделения ИБ-угроз на внешние и внутренние

Еще сравнительно недавно вопрос о целесообразности разделения угроз на внешние и внутренние можно было отнести к разряду надуманных. Так, по мнению директора по развитию бизнеса Центра информационной безопасности компании "Инфосистемы Джет" Евгения Акимова, такое разделение имеет вполне практический смысл, позволяя четче определиться с адекватными механизмами защиты. Более того, как полагает менеджер продукта компании "Код Безопасности" Иван Бойцов, разделение ИБ-угроз по типам и источникам актуально всегда — это общепринятая практика, поскольку универсальной защиты сразу от всех типов угроз не существует. Некоторые меры защиты могут быть общими как для внешних, так и для внутренних угроз, но большая часть из них все же направлена только на один тип нарушителя. В качестве примера г-н Бойцов приводит "Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" ФСТЭК России, где тоже разделяются угрозы, связанные с внешним или внутренним нарушителем, и дополнительно выделяются угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ. "Такое разделение угроз, — подчеркивает Иван Бойцов, — помогает определить характерные для данной компании уязвимости, оценить возможные риски и эффективнее применять соответствующие меры защиты".

Вместе с тем эксперты отмечают важные перемены в области ИБ. Ранее считалось, отмечает руководитель программ безопасности Microsoft в России Андрей Бешков, что внутренние сотрудники, которые могут представлять угрозу для предприятия своими намеренными действиями или халатностью, несмотря на то, что имеют больше возможностей, чем атакующие извне, все-таки надёжно контролируются, поскольку находятся внутри периметра. Однако в последние годы в связи с консьюмеризацией ИТ и распространением практики BYOD корпоративный периметр стал размываться, а то и полностью исчезать.

Подтверждая этот тезис, директор по решениям DeviceLock компании "Смарт Лайн Инк" Сергей Вахонин обращает внимание на то, что большинство сервисов социальных сетей, приложения облачных хранилищ, мессенджеры, используемые персоналом, попросту игнорируют корпоративные средства защиты и границы инфраструктуры: "Практически все сетевые приложения, созданные для удобства пользователей, для удовлетворения их социальных потребностей, функционируют абсолютно без какой-либо обратной связи с инструментарием корпоративной безопасности и контроля. Модель информационной безопасности потребительских приложений основывается на том, что все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь, который далеко не всегда является владельцем данных, будучи также сотрудником какой-либо организации". Все упомянутое выше позволяет Сергею Вахонину сделать вывод о том, что современная корпоративная модель ИБ, чтобы стать реально эффективной, должна быть информационно-центричной, опираться на совокупность контроля непосредственно данных и различных потоков их передачи и распространения.

По некоторым оценкам, внутренний сотрудник сегодня оказывается замешан в 80% ИБ-инцидентов. Довольно часто, по словам Андрея Бешкова, злоумышленники сначала захватывают идентификационные данные внутреннего сотрудника и уже затем действуют от его имени. Поэтому осталось мало смысла в разделении ИБ-угроз на внешние и внутренние. "В современных условиях, — считает он, — нужно вести проактивную ИБ-работу и разделять предприятие периметрами не только снаружи, но и внутри".

Схожей точки зрения придерживается и начальник отдела информационной безопасности ГК "Компьюлинк" Игорь Гавриш, который предлагает разделять внешние и внутренние угрозы лишь для обозначения класса применяемых для противодействия им технических решений, но не в рамках построения и модернизации системы информационной безопасности. Это, по его мнению, стало неактуально.

С тем, что наиболее опасные угрозы для корпоративной ИБ сегодня все чаще имеют гибридный характер, а потому стратегия обеспечения ИБ должна развиваться с учетом этой тенденции, согласен и Олег Глебов, менеджер по сопровождению корпоративных продаж "Лаборатории Касперского". В то же время, считает он, риски, связанные со злонамеренной инсайдерской активностью, резонно остаются исключительно внутренней проблемой и должны рассматриваться отдельно.

Внешние и внутренние угрозы — что опаснее?

Неоднозначность в подходах к разделению ИБ-угроз отражают и результаты недавнего исследования института SANS, показавшие, что 74% опрошенных ИБ-специалистов озабочены внутренними угрозами; 32% признают, что у них нет возможностей противостоять инсайдерам; 28% отметили, что в их организациях защита от инсайдеров вообще не считается приоритетной; 62% считают, что в планах реагирования на инциденты нет различия между внешними атакующими и внутренними.

В то же время в недавно опубликованных компанией Solar Security результатах исследований примерно 64% изученных ее специалистами ИБ-инцидентов, случившихся в I квартале 2015 г., были классифицированы как имеющие именно внутренние причины.

"Нехорошие" сотрудники своими нелегитимными действиями внутри предприятия могут причинять ему ущерб не только в виде утечек данных, но и в виде прямого воровства денежных и материальных ресурсов с использованием ИТ-систем. Бывают случаи, когда персонал организует реальные хакерские атаки внутри компании. Например, очень сложно противостоять угрозам, при реализации которых сотрудники компании вступают в сговор с третьими лицами. Так, если злоумышленнику крайне непросто внедрить вредоносный код в продакшн-систему (для этого требуется обойти массу барьеров и только после этого провести внедрение кода, который будет, к примеру, перенаправлять злоумышленнику информацию о заказе в интернет-магазине), то при возможности "договориться" с разработчиком приложения задача существенно упрощается. Обнаружение таких угроз требует выстроенных процессов безопасной разработки софта, о которых сейчас, увы, больше говорят, чем что-то реально делают.

По мнению Андрея Бешкова, внутренние угрозы находятся сейчас как бы ниже уровня чувствительности радара обнаружения атак: "Мало кто с ними реально разбирается и мало кто занимается защитой от них". Вместе с тем, учитывая то, что инсайдеры изначально имеют немалые полномочия доступа к ресурсам, они, по мнению Андрея Бешкова, опаснее внешних атакующих, поскольку с внешними угрозами индустрия ИБ, как он считает, уже более или менее научилась бороться.

Сергей Вахонин обращает внимание на разницу в подходах служб ИБ к противодействию внутренним и внешним угрозам. "Почему-то считается нормальным и правильным, — отмечает он, — внешним угрозам именно противодействовать, отражать внешние атаки, не допускать компрометации учетных записей и т. д. При этом в плане противодействия наиболее актуальной угрозе внутреннего характера — утечкам данных — зачастую подход обратный. Многие службы ИБ допускают утечки, преследуя только одну цель — зафиксировать утечку, а затем уже провести расследование инцидента".

Традиционно, считает Андрей Бешков, предприятия чрезмерно доверяют своим сотрудникам: "Их защита напоминает яйцо: снаружи более или менее твердая скорлупа, а внутри мягкая среда, и как только злоумышленник попадает в нее, он может делать все, что хочет".

Внутренние атаки, отмечает Иван Бойцов, остаются самыми опасными из-за размеров причиняемых ими прямых убытков. Это подтверждают ежегодные отчеты, публикуемые ISACA, PwC, Verizon и другими аналитическими компаниями. Происходит это потому, что потенциальный внутренний нарушитель знает, как устроены информационные системы, и зачастую располагает прямым доступом к конфиденциальной информации. Кроме того, внутреннему нарушителю заранее известно, какую информацию можно использовать для извлечения собственной прибыли.

Внешний же нарушитель должен потратить гораздо больше сил для атаки. Ему необходимо не только провести разведку и найти уязвимые места в системе защиты, но и определить ценность и локализацию полезных для него данных. С другой стороны, внешние атаки, по мнению Ивана Бойцова, опасны из-за косвенных убытков, так как часто они направлены на отказ в обслуживании публичной инфраструктуры организации. Такие атаки ведут к простоям в обслуживании клиентов, упущенной прибыли и репутационным потерям.

С этими выводами согласен ведущий консультант по ИБ компании R-Style Антон Зыков, который тоже считает, что угрозы, которые могут быть реализованы внутренним нарушителем, опаснее, так как он уже находится в офисе, в сети компании и обладает рядом экстра-возможностей: делегированным доступом, информацией, знаниями и способами их получения; по этой же причине внутренний пользователь часто становится первичной мишенью для внешних нарушителей.

Впрочем, есть и другое мнение. В отличие от процитированных выше экспертов Евгений Акимов полагает, что самые опасные ИБ-угрозы сегодня связаны с деятельностью внешних злоумышленников, чья активность в первую очередь направлена на кражу денег (например, через списание средств с банковских счетов с помощью вредоносной программы, подсаженной на компьютер главного бухгалтера). Жертвой такой атаки может оказаться любое предприятие — не обязательно банк.

Следует также помнить, что возможности внутренних и внешних нарушителей со временем эволюционируют. Сергей Вахонин и Игорь Гавриш обращают внимание на то, что внешняя атака, если преодолевает средства защиты корпоративного периметра, переходит в категорию внутренних угроз.

Современные кибератаки, добавляет Антон Зыков, проводятся сразу по нескольким векторам — как по внешним, так и по внутренним. Все чаще применяются сложные комплексные атаки типа таргетированных (APT-атаки). Поэтому наряду с традиционными инструмен-

Наши эксперты

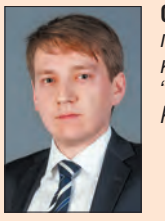
ЕВГЕНИЙ АКИМОВ, *директор по развитию бизнеса Центра информационной безопасности компании "Инфосистемы Джет"*

АНДРЕЙ БЕШКОВ, *руководитель программ безопасности Microsoft в России*

ИВАН БОЙЦОВ, *менеджер продукта компании "Код Безопасности"*

СЕРГЕЙ ВАХОНИН, *директор по решениям DeviceLock компании "Смарт Лайн Инк"*

ИГОРЬ ГАВРИШ, *начальник отдела информационной безопасности ГК "Компьюлинк"*



ОЛЕГ ГЛЕБОВ, *менеджер по сопровождению корпоративных продаж "Лаборатории Касперского"*

АНТОН ЗЫКОВ, *ведущий консультант по ИБ компании R-Style*

тами необходимо применять подходы, позволяющие адекватно противостоять новым вызовам. Такие подходы строятся на принципе "знай своего врага и знай себя". Смысл его заключается в способности компании прогнозировать поведение нарушителя и выявлять отклонения от нормальных среднестатистических признаков поведения своих пользователей. Для реализации этого принципа компания должна обладать информацией о том, что происходит во внешней среде и у себя внутри.

Слияние защиты от атак по внутренним и внешним векторам в защиту от единой, комплексной атаки произошло благодаря серьезным инвестициям компаний в средства защиты периметра сети, которые стали представлять собой эффективный заслон от внешних угроз, полагает Олег Глебов. С экономической стороны затраты на атаку "в лоб" могут оказаться для злоумышленников выше, чем возможная выгода в случае ее успеха. В результате злоумышленникам гораздо дешевле и проще использовать методы социальной инженерии, атаковать поставщиков и партнеров, использовать иные методы для того, чтобы попасть внутрь сети в обход средств защиты. В этом случае в помощь периметровой защите подключаются технологии не превентивного характера, а детектирующего, которые нацелены на максимально быстрое обнаружение любой подозрительной активности внутри инфраструктуры.

Защита от внешних и внутренних ИБ-угроз

Традиционно меры и средства защиты разделяются на организационные и технические. В обзоре мы тоже следуем такому разделению.

Организационные меры. Как отмечает Игорь Гавриш, организационные меры включают в себя, как минимум, назначение ответственного за ИБ в компании, контроль исполнения пользователем положений нормативно-правовых актов в области ИБ (НПА) по работе с информационными системами, регламентов и инструкций работы с подсистемами ИБ. Комплект НПА объединяют в рамках единой политики ИБ. Для выполнения требований законодательства по защите персональных данных в структуре НПА предусматривают дополнительные документы, запрашиваемые регуляторами в ходе проведения проверок.

Для обеспечения защиты от внутренних нарушителей в трудовых соглашениях с работниками компании прописывают пункты об ответственности за разглашение конфиденциальной информации, а также вводят режим коммерческой тайны, позволяющий, согласно законодательству, защитить интересы работодателя.

Говоря об организационных мерах, способствующих защите конфиденциальной информации от разглашения лицами, не являющимися сотрудниками компании, Игорь Гавриш предлагает в первую очередь заключать соглашения с контрагентами о неразглашении конфиденциальной информации, ставшей известной представителям контрагента в ходе договорных отношений. Для обеспечения доказуемости такого рода разглашений необходимо опять же ввести в компании режим коммерческой тайны, потому что в противном случае невозможно будет доказать, что являлось информацией, составляющей коммерческую тайну, а что — нет.

"Организационными мерами, — отмечает Антон Зыков, — невозможно воздействовать на поведение внешних нарушителей — субъектов, с которыми компания никак не связана формально. Зато их можно и нужно применять к внутренним пользователям, с тем чтобы они и сами не совершали нарушений, и не стали жертвами внешних нарушителей, попадаясь на всевозможные уловки. В первую очередь к таким мерам относятся повышение ИБ-осведомленности и четкая регламентация выполняемых бизнес-операций".

В организационных мерах обнаружить новые веяния, по мнению Ивана Бойцова, сложно, так как состав таких мер практически не меняется — разработка моделей угроз, нарушителей, защиты, составление политики безопасности, инструкций для сотрудников и регламентов работы, ввод режима коммерческой тайны и т. д. Все эти меры обязательны и необходимы для любой инфраструктуры и позволяют формализовать и упорядочить подход к защите информации.

Большую роль в защите от внутренних и внешних угроз играет обучение персонала вопросам защиты информации. Так как множество атак производится с помощью социальной инженерии, т. е. нетехническими методами, защиту от таких угроз можно выстроить только с помощью информирования сотрудников и обучения их работе по регламентам.

Если атака все же случилась, то первым лицом в реагировании, как отмечает Олег Глебов, в большинстве случаев становится вовсе не офицер ИБ, а сотрудник технической поддержки. Упущенное время оставляет злоумышленникам возможности для успешного завершения атаки и сокрытия следов. Поэтому правильная подготовка сотрудников технической поддержки в части ИТ-ориентированного обучения аспектам ИБ — важнейший элемент первичного детектирования и фильтрации ИБ-инцидентов от ИТ-событий.

Андрей Бешков рекомендует начинать строить ИБ-защиту вовсе не с внедрения технологических средств и инструментов. В первую очередь, полагает он, следует провести классификацию данных и процессов, чтобы понять, что именно предстоит защищать и каковы приоритетные направления защиты, поскольку без расстановки приоритетов все будет защищено одинаково плохо. При этом приоритеты должен определять не ИБ-специалист, а представители бизнеса компании. Следует выяснить, какие системы необходимо защищать в первую очередь, т. е. такие, без которых бизнес просто остановится, определить системы, на защите которых можно сэкономить или вообще не защищать.

В этом могут помочь инструменты, позволяющие понять, где и что хранится в корпоративной среде. Поможет также инвентаризация систем ИКТ-инфраструктуры на предмет выяснения того, где и что установлено, и в налаживании правильного управления обновлениями систем и изменениями конфигураций (с помощью соответствующих продуктов).

Затем предстоит решить, как сегментировать внутренние и внешние сети. Это нужно сделать обязательно, потому что компрометация инфраструктуры в длительной перспективе неизбежна, следовательно, нужно строить изолированные отсеки, как на кораблях или подводных лодках, дабы повысить живучесть инфраструктуры и сервисов в целом.

В особо защищаемые сегменты нужно вынести жизненно важные для бизнеса системы и решить, из каких сегментов сети к ним будет доступ — будут ли, например, эти системы доступны сотрудникам с мобильными устройствами или только тем, которые пользуются стационарными ПК из внутренней сети.

После этого надо постараться минимизировать число привилегированных пользователей и внедрить ролевой доступ к системам. Затем можно начинать внедрять системы протоколирования действий привилегированных пользователей и ограничить количество действий, доступных для выполнения ими.

Практически все упомянутые меры защиты актуальны и для внешних, и для внутренних атак. "В условиях, когда атаки стали выполняться сразу по нескольким векторам, стоит избавиться от веры в единый периметр и создавать несколько периметров и сегментов сети для минимизации ущерба, — считает Андрей Бешков. — Вера в неуязвимость инфраструктур губительна. Это значит, что особое внимание стоит уделить тестированию инфраструктуры на проникновение".

Нужно также спланировать регулярный поиск, возможно, уже происходящих компрометаций систем, учитывая, что с момента компрометации до момента ее обнаружения проходит в среднем более 200 дней. За это время атакующие надежно и удобно обустраиваются в захваченных инфраструктурах. В результате изгонять их оттуда очень сложно, поэтому чем раньше обнаруживается компрометация, тем легче бороться с атакующими. В этом может помочь внедрение систем класса SIEM и систем анализа поведения инфраструктуры и пользователей. На вершине всей архитектуры защиты должны располагаться меры и средства по обеспечению непрерывности бизнеса, включающие в себя тренинги по реагированию на инциденты и восстановлению бизнеса после инцидента.

Технические средства. До тех пор, полагает Евгений Акимов, пока внешние и внутренние злоумышленники не начинают работать в связке, механизмы защиты от них, как правило, выстраиваются разные.

Для противодействия внешним и внутренним угрозам применяют специализированные средства защиты, начиная с систем предотвращения вторжений и межсетевых экранов и завершая комплексами решений, направленными на противодействие таргетированным атакам: песочницы, системы управления ИБ и событиями ИБ, веб-шлюзы, шлюзы электронной почты, средства мониторинга действий администраторов и других привилегированных пользователей, контроль выполняемых транзакций и поведенческих моделей, контроль уязвимостей инфраструктурных компонентов и бизнес-приложений и др.

В связи с постоянными изменениями (прежде всего во внешней среде) данные для таких средств нужно поддерживать в актуальном состоянии, для чего должен быть выстроен четкий процесс постоянного мониторинга на базе служб реагирования на инциденты (SOC) с применением аналитических данных из внешних и внутренних источников (Threat Intelligence).

Против внутренних угроз упомянутые выше решения применяются редко — для этого прежде всего используются хорошо известные системы управления доступом, системы предотвращения утечек данных, а теперь и фрод-машины, выявляющие мошеннические схемы в различных бизнес-операциях, начиная от воровства на кассовых аппаратах и завершая нарушениями в логистике.

Подход к защите от внешних угроз, отмечает Иван Бойцов, постепенно смещается в сторону усиления контроля защищенности. На рынке появляются новые инструменты для проверки политики безопасности, правильности настройки оборудования и проведения анализа защищенности.

На фоне растущего числа и качества угроз и, как следствие, количества и усложнения применяемых средств защиты на первый план выходят задачи управления всей корпоративной ИБ-системой. Вести мониторинг и управлять всеми защитными механизмами, внедренными в компании, становится затруднительно и дорого. В то же время несовместимость и разрозненность средств защиты информации (СЗИ) сами по себе тоже создают дополнительные угрозы ИБ. Поэтому сейчас вендоры стремятся совмещать защитные механизмы в одном продукте и предоставлять заказчику возможность работать с ними через единый интерфейс управления.

Комплексный подход к защите, считает Иван Бойцов, в первую очередь выражается в корреляции событий безопасности и интеграции различных механизмов защиты между собой. Современная система защиты должна строиться не на разрозненных средствах защиты, способных работать только в своей узкой области, а на комплексных продуктах, умеющих сопоставлять между собой различные события и позволяющих вырабатывать комплексную реакцию в зависимости от общей ситуации.

Олег Глебов обращает внимание на рост востребованности систем автоматизации процессов расследования инцидентов (форензика). Эти системы не являются превентивными, но, относясь к средствам апостериорной защиты, предлагают мощный инструментарий для постоянного сбора данных и проведения глубоких расследований на постоянной основе или в случае уже произошедших инцидентов (неважно, внутренних или внешних).

К сожалению, сегодня, отмечает Игорь Гавриш, только небольшое число компаний имеют проработанную стратегию, используют такие комплексные решения, как сбор и корреляция событий ИБ (из источников внешних и внутренних угроз), комбинированные решения сетевой безопасности (защиты от внешних и внутренних угроз). По его мнению, комплексный подход к организации корпоративной ИБ — сущность достаточно сложная, система менеджмента ИБ для обеспечения комплексности должна быть частью общей системы управления компанией и должна основываться на управлении бизнес-рисками для создания, внедрения, эксплуатации, мониторинга, анализа, поддержания и улучшения ИБ.

Нельзя также забывать, что обеспечение ИБ — непрерывный процесс. Пока существует сама информация, требующая защиты, система менеджмента ИБ (СМИБ) должна основываться на известной модели PDCA (Plan-Do-Act-Control, планирование — осуществление — проверка — действие).

Роль государственного регулирования при построении защиты от внешних и внутренних угроз

Государственное регулирование в области ИБ, независимо от происходящих в экономике и политике процессов, по мнению Ивана Бойцова, играет важную роль в любое время, так как защищает интересы государства и его граждан. Конечно же, органы регулирования ориентируются на общую политику государства в области кибербезопасности и в других смежных областях (например, импортозамещении). В то же время он считает, что основное влияние на регуляторов и формирование нормативно-правовой базы оказывает развитие ИТ, появление новых векторов атак и другие технические изменения.

Обращаясь к конкретным направлениям регулирования, Олег Глебов отмечает, что жесткие требования сертификации ПО, как минимум, показали свою пользу в борьбе с незадекларированным функционалом (бэкдорами, закладками и т. п.). Резонно, на его взгляд, рассмотреть возможность для промышленных предприятий и энергетики иметь средства сбора данных о состоянии критичных процессов в технологических сетях, которые могли бы передавать эту информацию, например, в государственные центры мониторинга критичной инфраструктуры. Это, по его мнению, позволило бы не только снизить время обнаружения готовящихся внешних атак на промышленные инфраструктуры, но и проводить расследования постфактум о причинах возникновения инцидентов.