Исследование защищенности ресурсов
и трудности выбора методик

Артем САВЧУК,
технический директор компании «Перспективный мониторинг»

Подходы к тестированию системы ИБ – один из актуальных вопросов для профессионалов, отвечающих за обеспечение защиты информационных ресурсов. При обсуждении доступных вариантов решений специалисты изучают возможность исследования защищенности информационных систем. При этом объектами исследования могут быть документы, процессы, процедуры, непосредственно системы, сотрудники – все, что может оказывать влияние на информационную безопасность и быть уязвимым элементом системы. От задач конкретного проекта зависит выбор: проводить пентест, использовать методы социальной инженерии или провести аудит систем на соответствие требованиям регуляторов. В чем различие данных типов работ, кому стоит регулярно проводить исследования защищенности, как оценить полученные результаты?

Когда заказчики приходят с запросом на конкретный вид работ – тестирование, аудит, анализ защищенности, – в процессе диалога зачастую выясняется, что им нужна совсем иная услуга или даже их набор. Для общего описания комплекса методов и работ, которые позволяют оценить уровень защищенности информационных систем организации на основе результатов исследования объектов, мы используем базовый термин «исследование защищенности». Выбор методики (пентест, социальная инженерия, аудит систем на соответствие требованиям регуляторов) зависит от задач конкретного проекта.

Аудит ИБ или пентест

Оценка соответствия (аудит) ИБ – это систематический, независимый и документируемый процесс получения свидетельств аудита деятельности организации по обеспечению ИБ и установления степени выполнения в организации установленных критериев аудита ИБ. Такими критериями могут служить требования нормативных документов регуляторов в области защиты информации, нормативных актов отраслевых регуляторов, документов национальной системы стандартизации, внутренних нормативных документов организаций. В качестве примеров можно привести следующие:

- нормативные документы ФСТЭК:
  - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 № 17;
  - Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25.12.2017 № 239;
  - Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14.03.2013 № 31;
  - Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18.02.2013 № 21;
- нормативные акты Банка России:
  - Положение Банка России № 683-П от 17.04.2019;

- Положение Банка России №№ 821-П от 17.08.2023;
- Положение Банка России № 802-П от 25.07.2022;

- национальные стандарты Российской Федерации:
  - ГОСТ Р 57580.1–2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер;
  - ГОСТ Р 57580.3–2022 Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения;
  - ГОСТ Р 57580.4–2022 Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер;
  - ГОСТ Р ИСО/МЭК 27001–2021 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Использование требований тех или иных документов в качестве критериев аудита информационной безопасности определяется его целями. Аудиторская группа изучает информационную инфраструктуру и оценивает, какие требования и меры реализованы, если реализованы, то какими средствами и насколько полно. В рамках аудита ИБ применяются методы изучения документации, интервьюирования уполномоченных лиц и наблюдение за выполняемой деятельностью. То есть исследование осуществляется без вмешательства в информационную систему и систему обеспечения информационной безопасности. Результаты аудита ИБ позволяют определить степень полноты реализации требований и мер ИБ и при необходимости понять, соответствует ли система обеспечения информационной безопасности организации или информационной системы регуляторным требованиям.

Вместе с тем потенциальные клиенты часто заказывают проведение пентеста (тестирование на проникновение) той или иной организации. При этом очень удивляются, когда их просят уточнить, что конкретно требуется получить в качестве результата. Многие из них уверены, что пентест – единственный вид работ, который позволяет проверить уровень безопасности информации организации.

Сравнение методов

Основное отличие тестирования на проникновение от аудита ИБ заключается в моделировании атаки злоумышленника на информационную систему. То есть исследование может осуществляться с вмешательством (по решению владельца информационной системы) в информационную систему и систему обеспечения информационной безопасности. Оно включает в себя анализ информационной системы и системы обеспечения информационной безопасности на наличие потенциальных уязвимостей, которые могут позволить реализовать атаку, и может включать в себя эксплуатацию выявленных уязвимостей системы.

Основное отличие тестирования на проникновение от аудита ИБ заключается в моделировании атаки злоумышленника на информационную систему.

На самом деле пентест – лишь один из вариантов, причем не самый распространенный. На практике большинству заказчиков подходит анализ защищенности – вид работ, при котором поверхность компьютерной атаки проверяется максимально широко, чтобы охватить наибольшее количество векторов атак.

Пентест, напротив, сужает количество векторов, ограничиваясь только максимально перспективными с точки зрения проникновения. Таким образом, пентест – это атака «в глубину», а анализ защищенности – «в ширину».

В некоторых ситуациях необходимо, например, проведение атак методами социальной инженерии: «разбрасывание» вредоносных флешек в местах скопления сотрудников, распространение фишинговых писем, звонки, в ходе которых исследователи уговаривают сотрудников сообщить чувствительную информацию или выполнить определенные действия. А если у предприятия есть свой SOC, то может представлять интерес не столько атака, сколько оценка работы защищающихся.

Результаты тестирования на проникновение позволяют понять, насколько оптимально спроектированы информационная система и система обеспечения информационной безопасности, насколько хорошо функционирует процесс управления обновлениями, насколько адекватно ландшафту угроз сконфигурированы средства защиты информации, насколько добросовестно персонал служб ИТ и ИБ выполняет свои обязанности.

Таким образом, противопоставлять эти два метода оценки защищенности информационных систем нельзя. Они органично дополняют друг друга. И если аудит ИБ дает комплексную оценку соответствия системы обеспечения

информационной безопасности тому или иному набору требований, то тестирование на проникновение позволяет точечно оценить эффективность применяемых мер защиты информации в условиях их естественной деградации относительно постоянно изменяющего ландшафта угроз ИБ.

Взвесить «за» и «против»

Ряд предприятий (например, кредитные организации, субъекты критической информационной инфраструктуры) обязаны проводить работы по улучшению безопасности – пентест или анализ защищенности в соответствии с законодательными требованиями.

Но и среди компаний, не подпадающих под обязательные законодательные требования либо положения нормативных правовых актов РФ, довольно много организаций, которые понимают, что цена ущерба от реализации компьютерной атаки или инцидента очень высока. К таковым можно отнести интернет-магазины, крупные интернет-порталы и социальные сети.

Можно ли пренебречь тестированием системы ИБ и, как следствие, реализацией смежных рисков предприятия? Да, если тщательно посчитать бизнес-риски: просто оценить их стоимость. Достаточно прикинуть ущерб от нарушения работы интернет-магазина за час, день либо стоимость компрометации информации в случае утечки данных, составляющих коммерческую тайну. В таком же порядке определяется цена ущерба при блокировке рабочих станций всех сотрудников регионального филиала, когда важные данные на них зашифрованы, а резервное копирование не осуществлялось.

Несмотря на то, что не все риски могут реализоваться и привести к перечисленным последствиям, стоит получить условную сумму и сравнить ее со стоимостью проведения работ по повышению системы безопасности предприятия. В последнее время все большую популярность набирает и так называемое страхование киберрисков. В 2023 г. пострадавшие компании в России уже получали первые страховые выплаты по этому виду страхования.

В последнее время все большую популярность набирает и так называемое страхование киберрисков. В 2023 г. пострадавшие компании в России уже получали первые страховые выплаты по этому виду страхования.

Гарантии защиты

К сожалению, невозможно считать компанию защищенной после проведения пентеста или другого исследования. Эти мероприятия значительно повышают, но не гарантируют защищенность информационной системы организации от злоумышленников.

На следующий день в Интернете может выйти статья с описанием метода обхода выбранного средства защиты информации, злоумышленники найдут новую уязвимость для сервера, а уборщице организации заплатят годовую зарплату, чтобы она подключила USB-устройство к компьютеру финансового директора.

Опасностей – множество, и для специалистов в сфере ИБ это ежедневная рутина. Чтобы избежать негативного сценария развития событий, нужно тщательно к нему готовиться. Должны быть внутренние документы и регламенты, описывающие действия в различных ситуациях. Для этого выполняются работы по анализу защищенности, проводится пентест, чтобы посмотреть, как потенциальные атакующие будут видеть и взламывать защиту предприятия. Злоумышленники, которые во многом будут повторять путь исследователей, быстро утратят интерес и пойдут искать более простую цель.

Но есть нарушители, которые не остановятся, если их цель – атака на конкретную организацию. Если нарушитель понимает, зачем он атакует, то компания должна точно понимать, зачем защищаться.

Чудеса социальной инженерии

Все чаще злоумышленники используют методы социальной инженерии для проникновения в информационные системы организаций, поэтому важно также регулярно проводить обучение сотрудников.

Приведем несколько показательных случаев из нашей практики. В ходе одного исследования проверялась организация сети Wi-Fi. Одной из таких проверок было создание поддельной сети на устройстве исследователя с тем же именем, что и настоящая корпоративная точка доступа. Был даже повторен интерфейс портала, через который сотрудники получали доступ в интернет. Обычно в такую ловушку персонал попадает нечасто, но в ходе этой работы один сотрудник с необычным упорством полтора часа пытался получить доступ в «интернет» через нашу сеть – вводил вручную огромное количество паролей (мы не могли подтвердить пароль, поэтому на любую его попытку устройство отвечало, что пароль неправильный).

С упорством, достойным лучшего применения, он вводил и свои корпоративные учетные данные и, видимо, пытался ввести учетные данные от внутренних сервисов, даже попробовал такие редкие способы аутентификации, как вход по сертификату – в общем, обеспечил нас достаточным количеством чувствительной информации. Мы специально выключили поддельную сеть через некоторое время, чтобы сотрудник перестал тратить время и занялся прямыми рабочими обязанностями.

В ходе другой проверки нам нужно было попасть на территорию предприятия. Сработал стандартный сценарий: исследователь представился проверяющим из вымышленной организации «ОблТоргМетАлмазГазНефть в сфере информационных технологий» и вместо проверки документов его пропустили на территорию, отвели к главному системному администратору, который пустил за свой рабочий компьютер и сообщил пароль для входа. Все оказалось настолько просто, что в это было даже сложно поверить.

Обязательные мероприятия

Для некоторых организаций и предприятий аудит ИБ и тестирование на проникновение – обязательные мероприятия. В частности, для финансовых организаций Банк России устанавливает периодичность проведения этих мероприятий. Аудит ИБ может проводить только независимая организация – лицензиат ФСТЭК, имеющая лицензию на услуги по технической защите конфиденциальной информации. По результатам таких мероприятий финансовые организации отчитываются перед Банком России, заполняя установленные отчетные формы.

ФСТЭК России пока не предъявляет требований относительно периодичности проведения аудита ИБ и тестирования на проникновение. Однако, исходя из Информационного сообщения ФСТЭК России «Об утверждении методического документа ФСТЭК России «Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации», ФСТЭК России планирует ввести в действие нормативные правовые акты, устанавливающие требования по оценке показателя текущего состояния технической защиты информации и обеспечения безопасности объектов КИИ.

При проведении аудита ИБ возникает вопрос: как оценить степень реализации требований, чтобы можно было обеспечить сопоставимость результатов, особенно в условиях привлечения для выполнения работ по аудиту ИБ различных исполнителей. Для этого нужны методики проведения аудита ИБ с учетом различных нормативных документов.

Аудит ИБ может проводить только независимая организация – лицензиат ФСТЭК, имеющая лицензию на услуги по технической защите конфиденциальной информации.

Банк России параллельно с ГОСТ Р 57580.1–2017 подготовил ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». Этим документом в настоящее время руководствуются организации-оценщики для проведения аудита ИБ по требованиям ГОСТ Р 57580.1 в финансовых организациях. Кроме того, для каждого из нормативных актов, по выполнению требований которых финансовые организации должны отчитываться перед Банком России, также подготовлены соответствующие методические рекомендации.

В мае 2024 г. ФСТЭК утвердил «Методику оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Документ позволяет определить показатель, характеризующий текущее состояние технической защиты информации, не составляющей государственную тайну, и обеспечения безопасности значимых объектов критической информационной инфраструктуры РФ, его нормированное значение и порядок расчета.

Методика ориентирована на оценку состояния защиты информации в государственных органах, органах местного самоуправления, организациях и степени его соответствия минимально необходимому уровню защиты информации от типовых актуальных угроз.

Методикой предусмотрен минимальный уровень мер, которые организации обязаны применять для защиты информации. Они регламентированы нормативными правовыми актами Российской Федерации и минимально достаточны для блокирования типовых актуальных угроз безопасности информации. Методика прозрачна и построена на основе иерархии групповых и частных показателей защищенности. В документ включен набор частных показателей защищенности, позволяющий оценить реализацию достаточно ограниченного набора мер Приказов ФСТЭК № 17, 21, 239, 31, что оправдано с точки зрения универсальности методики. Пока данная методика может применяться по решению организаций либо в случае поступления запроса со стороны ФСТЭК. ■