ТЕМА НОМЕРА

ИНТЕРВЬЮ БРАЛ: АНДРЕЙ КАРОЛИК (KAROLIK@ITSPECIAL.RU)

Константин Гавриленко,
управляющий директор компании «Архонт»

Андрей Владимиров,
глава отдела безопасности компании «Архонт»

«КАК И В МЕДИЦИНСКОЙ ПРАКТИКЕ, БОЛЕЗНЬ ЛЕГЧЕ ВЫЛЕЧИТЬ НА НАЧАЛЬНОЙ СТАДИИ»

«АРХОНТ» (ЛОНДОН, ВЕЛИКОБРИТАНИЯ; WWW.ARHONT.COM) — КОМПАНИЯ, ЗАНИМАЮЩАЯСЯ ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ ПЕРЕДАЧИ И ХРАНЕНИЯ ИНФОРМАЦИИ. СФЕРА ДЕЯТЕЛЬНОСТИ ОХВАТЫВАЕТ ВСЕ АСПЕКТЫ СЕТЕВОЙ ЗАЩИТЫ И БЕЗОПАСНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ: ПРОЕКТИРОВАНИЕ УКРЕПЛЕННЫХ СЕТЕЙ, ПОИСК И АНАЛИЗ УЯЗВИМОСТЕЙ, ТЕСТИРОВАНИЕ НА ВОЗМОЖНОСТЬ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И СООТВЕТСТВИЕ МЕЖДУНАРОДНЫМ СТАНДАРТАМ СЕТЕВОЙ БЕЗОПАСНОСТИ, ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ, БЕЗОПАСНОЕ ПРОГРАММИРОВАНИЕ, СУДЕБНАЯ ЭКСПЕРТИЗА В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВЕРИФИКАЦИЯ И ПРОВЕРКА ДОСТУПА ДЛЯ СЕРВЕРОВ И ПОДКЛЮЧЕННЫХ К ИНТЕРНЕТУ РАБОЧИХ СТАНЦИЙ, ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННОГО ВТОРЖЕНИЯ, ПРИНЯТИЕ ОТВЕТНЫХ МЕР И ПРОВЕДЕНИЕ СООТВЕТСТВУЮЩЕГО РАССЛЕДОВАНИЯ. СРЕДИ ПЕЧАТНЫХ РАБОТ СОТРУДНИКОВ КОМПАНИИ: «WI-ФУ: «БОЕВЫЕ» ПРИЕМЫ ВЗЛОМА И ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ" И «СЕКРЕТЫ ХАКЕРОВ: СЕТИ CISCO».

Корректно ли сравнивать внутренний аудит с регулярной профилактикой? И почему бы не объединить внутренний и внешний аудит, назвав все одним словом «аудит» и проводя одновременно? Или есть принципиальные различия, из-за которых это невозможно в принципе?

Константин Гавриленко:

Вполне корректно, и не только внутренний аудит можно сравнить с профилактикой. Последняя подразумевает предохранение. А основной целью любого аудита безопасности является как раз выявление слабых мест инфраструктуры или процессов и рекомендации по их укреплению для предохранения от возможного проникновения или получения доступа к конфиденциальной информации. Как видите, параллель возникает сама собой. Как и в медицинской практике, болезнь легче вылечить на начальной стадии, а еще лучше попытаться предотвратить, например посредством разработки системы мер предупреждения возникновения и воздействия факторов риска, так называемой первичной профилактики.

Естественно, есть и различия, но недостаточно принципиальные для невозможности их объединения. Скорее, эти два типа аудитов дополняют друг друга, как и навыки, необходимые для их проведения. Разделение делается для удобства клиента, это своего рода маркетинговый ход. Типична ситуация, когда начальник ИТ-отдела может здраво оценить квалификацию своих сотрудников, провести поверхностный анализ и решить, в каких областях ему нужна профессиональная сторонняя консультация. Компания, которая не разделяет сервисы и недостаточно гибка, чтобы удовлетворить пожелания клиентов, долгое время не продержится на рынке.

Кому вообще нужен внутренний аудит?

Андрей Владимиров:

Непросто обозначить общие характеристики компаний, которым он необходим, или причины, которые могут сподвигнуть их на проведение внутреннего аудита. Такие компании можно условно разделить на три категории:

1. те, где руководство хочет проверить работу своих сотрудников;
2. организации, которым в силу различных причин нужна сторонняя помощь;
3. предприятия, проходящие различные сертификации.

Внутренний аудит важен для организаций, которые напрямую зависят от корректной работы ИТ-инфраструктуры, чей бизнес может остановиться при умышленной дезорганизации работы узлов и сетей. Допустим, компания занимается телемаркетингом и у них установлена система VOIP-телефонии без дублирующей POTS-системы. Злонамеренные действия, направленные на остановку этой системы, парализуют деятельность всей компании. Соответственно от корректного функционирования системы зависит успех организации и основные приоритеты внутреннего аудита.

Любой аудит безопасности – достаточно нетривиальная задача в силу различий между компаниями, их подхода к построению ИТ-инфраструктуры и обеспечению безопасности. Как решать подобное уравнение с множеством неизвестных?

Константин Гавриленко:

Абсолютно верно, что каждая ИТ-инфраструктура имеет свои особенности и требует индивидуального подхода. В то же самое время ключевые компоненты сети, относящиеся к безопасности, зачастую схожи. Как раз на тестировании этих узлов во многом и концентрируется внимание аудитора. А еще много общего у систем управления сетями. К примеру, какая аппаратная часть от Cisco не использовалась бы, CiscoWorks везде CiscoWorks и будет использовать одни и те же протоколы мониторинга и удаленного управления — SNMP, CDP и т. д. Дальше все зависит от выбранной методологии и опыта аудиторов. В случае, когда аудитору попадается какая-то новая технология, конечно, больше времени нужно потратить на ее изучение. Как правило, это делается после согласования контракта и перед самим аудитом, так называемое «домашнее задание».

Что сложнее, подготовка к аудиту и сбор исходных данных для его начала или непосредственно сам процесс проверки? Какие обычно сроки проведения внутреннего аудита?

Андрей Владимиров:

Сроки варьируются, несмотря на то, что общий подход к решению задачи более или менее одинаков. Существует огромное количество нюансов для каждой конкретной компании, что, в свою очередь, влияет на время, затрачиваемое на исследование определенного компонента сети. Сравнивать подготовку к аудиту и непосредственно сам аудит, на мой взгляд, не имеет особого смысла. При наличии постоянной загруженности, время, необходимое на подготовку да и на сам аудит, уменьшается в связи с приобретаемым опытом как в техническом плане, так и в умении общаться с людьми. А все проблемы по сути дела выявляются в ходе аудита, ибо «теоретический» анализ схем сетей, конфигурационных файлов устройств, политик и руководств безопасности и так далее все равно является его частью. А некоторые про-

ИНТЕРВЬЮ БРАЛ: АНДРЕЙ КАРОЛИК (KAROLIK@ITSPECIAL.RU)

блемы обнаруживаются и после проведения аудита как такового, в ходе сопоставления и анализа полученных результатов.

Сколько может стоить внутренний аудит и что влияет на конечную стоимость проводимых мероприятий?

Константин Гавриленко:

Конечная стоимость проводимого аудитав основном зависит от количества человекочасов, затраченных на сам аудит. После оглашения и согласования задания делается оценка его сложности, составляется приблизительная смета затрат времени консультантов, определяются необходимые квалификации, высчитывается проформа фактуры стоимости работы, и все это передается на утверждение заказчику. Стоимость аудита зависит от размера тестируемой инфраструктуры и ее комплексности. Могут играть роль и дополнительные факторы, такие как установленные меры защиты сетей. Скажем, клиент хочет, чтобы тестирование проводилось максимально тихим образом с постепенным повышением его «шумности» для проверки «чувствительности» распределенной системы обнаружения несанкционированного доступа. Разумеется, это увеличит и продолжительность аудита, и требования к умениям аудиторов, и затраченные на тестирование усилия.

Что клиент имеет на выходе после проведенного внутреннего аудита?

Андрей Владимиров:

Результатом успешно проведенного внутреннего аудита безопасности является отчет, в котором подробно описывается методология, использованная при проведении аудита, все найденные уязвимости с прикладными примерами и подробные рекомендации по устранению этих уязвимостей. Также отмечаются другие, непосредственно не связанные с безопасностью проблемы, которые были обнаружены при проведении аудита, например мисконфигурации DNS и петли маршрутизации. Мы любим повторять известную фразу Дана Каминского: «Стабильность и безопасность сети — две стороны одной медали», и это действительно так. Кроме того, полноценный отчет должен включать в себя оценку риска и необходимого уровня атакующего на каждую найденную уязвимость, содержать анализ общего уровня безопасности сети. В ходе последнего часто выявляются административные проблемы: отсутствие четких политики и стандартов безопасности, несогласованность систем управления безопасностью сетей, когда конфигурация устройств и систем производится разными администраторами с разным уровнем знаний и отношением к их защите, и т. д. Подобного рода проблемы, равно как и ранее неизвестные дыры, не обнаружит ни один автоматический сканер уязвимостей. И обычно именно они являются первоисточником остальных, более частных прорех. Все эти вещи обсуждаются с ИТ-дирекцией и системными администраторами клиентской компании после того, как они ознакомились с отчетом, и в ходе этого обсуждения определяются приоритеты по устранению найденных проблем и находятся наиболее приемлемые решения.

Обычно внутренний аудит – это некий рекомендательный документ или же комплекс мер по обнаружению и устранению наиболее важных недостатков в ИТ-инфраструктуре клиента?

Константин Гавриленко:

Внутренний аудит — это процесс, а вот следствие этого процесса — как раз отчет,

Индивидуальный подход

Некоторые проблемы, возникающие при проведении внутреннего аудита, закладываются еще на этапе разработки и согласования методики аудита. Порой до 50% успеха проекта обеспечивает детальная методика проведения аудита. Именно она определяет основные составляющие проекта: схему выполнения, участников, состав собираемых данных, результат. Поэтому этап формирования и согласования методики обследования является ключевым в любом аудите. Даже если используются типовые методики, их необходимо пересматривать и согласовывать с заказчиком работ перед каждым проектом.

содержащий описание прорех безопасности в ИТ-инфраструктуре клиента и рекомендации по их устранению. Например, во время аудита консультант обнаружил возможность переключения одного из портов коммутатора в TRUNK-режим и перехвата трафика со всех VLAN'ов. Соответственно в отчет вписываются детали обнаруженной уязвимости, небольшой анализ того, как она может повлиять на общий уровень безопасности, и что нужно сделать для устранения этой уязвимости.

Когда проведение внутреннего аудита можно или нужно обеспечить своими силами, а когда проще и разумнее обратиться к независимому аудитору?

Андрей Владимиров:

Если бюджет позволяет, то разумней обратиться к независимому аудитору. Аудит внутренней безопасности — занятие весьма дорогостоящее, поэтому резонно использовать свои силы только для проведения мини-проверок, в перерыве между основными аудитами с привлечением сторонних специалистов. Когда требования к безопасности особенно сильны и правление компании может выделить практически неограниченный бюджет, имеет смысл создать внутреннюю службу аудиторов. Так поступают многие транснациональные корпорации. Но даже им приходится прибегать к сторонним консультациям для решения каких-то узконаправленных задач, например связанных с беспроводной безопасностью и другими специфическими задачами. В любом случае важен фактор независимости аудита, его свободы от внутрикорпоративных отношений и интриг, беспристрастный взгляд со стороны.

Элементарный пример. Если ИТ-специалисты компании обнаружат прорехи в защите систем, в которых сами же и виноваты, будут ли они рады докладывать об этом вышестоящему начальству? И будут ли вообще их устранять, если это «лишняя» работа, за которую никто не доплатит, а пока еще «никто ничего не взломал», и вообще «все это внутри, прикрыто межсетевым экраном»? Не умолчат ли они о проблемах и не оставят ли все как есть, положившись на авось?

Как оценить эффективность проведенного аудита? Чтобы не возникало ситуации, когда внутренний аудит выявит только часть существующих проблем, тем самым только усугубив ситуацию.

Константин Гавриленко:

На мой взгляд, нет полноценной и равнозначной системы оценки эффективности аудита. Невозможно «выловить» абсолютно все уязвимости, включая ранее неизвестные, за короткий срок, обычно отведимый под аудит. Если опустить аспекты личных симпатий и откатов, то, выбирая аудиторскую компанию, в основном следует оценивать ее предыдущий опыт нестандартного подхода к решению задач, что проявляется в найденных новых уязвимостях, в собственных исследовательских работах, новых методологиях и т.д. Также стоит оценить список клиентов и тип ранее проделанной работы приглашаемого аудитора, не лишним будет запросить рекомендации.

Если внутренний аудит выявил только часть имеющихся проблем, это ни в коем случае не усугубляет ситуацию, а наоборот, поднимает «планку безопасности». Процесс проведения аудитов весьма стандартизирован и существует множество методологий, описывающих различные его аспекты. С другой стороны, поиск новых уязвимостей — процесс творческий. Способность проанализировать множество мелких уязвимостей, воссоздать общую картину и объединить незначительное в единое, которое позволит получить вожделенный доступ, на мой взгляд, это то, что отличает настоящего пентестера от тех, для кого это просто подневольная работа или дополнительная нагрузка от начальства. it