АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD. И КОНСТАНТИН ГАВРИЛЕНКО, MD ARHONT LTD

ОБЩАЯ ПРОВЕРКА БЕЗОПАСНОСТИ при проведении внутренних аудитов

В БОЛЬШИНСТВЕ ОРГАНИЗАЦИЙ ПОД СЛОВОСОЧЕТАНИЕМ «ВНУТРЕННИЙ АУДИТ БЕЗОПАСНОСТИ» В ПЕРВУЮ ОЧЕРЕДЬ ПОДРАЗУМЕВАЮТ, ЕСЛИ НЕ ФИЗИЧЕСКУЮ ПРОВЕРКУ ОФИСА НА ПРЕДМЕТ ЖУЧКОВ И ПОПЫТОК ПРОНИКНОВЕНИЯ ЛЮДЬМИ ИЗ ОРГАНОВ, ТО, КАК МИНИМУМ, ПРИХОД СЕРЬЕЗНОГО ВИДА «АЙТИШНИКА» В КОСТЮМЕ ОТ ОДНОЙ ИЗ КРУПНЫХ КОНСАЛТИНГОВЫХ КОНТОР. МНОГИЕ СИСАДМИНЫ, БЕЗ СОМНЕНИЯ, ВПАДАЮТ В ТИХИЙ УЖАС И РВУТ НА СЕБЕ ВОЛОСЫ В ОЖИДАНИИ ТОГО, ЧТО КОНСУЛЬТАНТ НАЙДЕТ СЕРЬЕЗНЫЕ ПРОРЕХИ В МЕРАХ ЗАЩИТЫ ИЛИ ХОТЯ БЫ НЕБЕЗОПАСНЫЕ ПОСЛАБЛЕНИЯ, СДЕЛАННЫЕ ДЛЯ УДОБСТВА ПОЛЬЗОВАТЕЛЕЙ.

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD, И КОНСТАНТИН ГАВРИЛЕНКО, MD ARHONT LTD

Необходимость обеспечения внутренней безопасности сети чаще всего недооценивается администраторами. Даже если какие-то опции, связанные с безопасностью, изначально были запланированы и установлены, то позже по просьбе пользователей они убираются для упрощения процесса «общения» с компьютером и сетью. Нередки случаи, когда средства обеспечения внутренней безопасности вообще отсутствуют и пользователь открывает вместо какого-то конкретного фолдера доступ ко всему диску, устанавливая разрешения на чтение/запись, минуя списки контроля доступа, доверительные отношения и настройки безопасности по установке. Большинство такого рода дополнений для удобства работы значительно понижает требования к навыкам нападающего и ставит целостность сетей и систем под угрозу.

В толково спроектированной и настроенной сети большинство пользователей не нуждается в доступе и не должно иметь его к машинам других пользователей, за исключением ресурсов, специально предназначенных для совместной работы. Они также не должны иметь доступа к административным функциям и ресурсам, сетевым устройствам и т.д. Однако недостаточная компьютерная грамотность администраторов и пользователей часто не позволяет настроить и поддерживать сеть на требуемом уровне гибкости и удобства для эффективного ведения основного бизнеса организации. Внутренние сети по определению не могут иметь максимальную безопасность, поэтому они и отделены от Интернета и/или разделены на виртуальные локальные сети согласно административным требованиям. Их пользователи наделены приблизительно одинаковыми правами и по идее не должны быть заинтересованы в атаках друг на друга или на центральные системы и ресурсы. Но подобный подход, когда системный администратор, которого часто начальство не воспринимает как человека, приносящего непосредственный доход для компании, вынужден прогибаться под прихоти пользователей, увы, встречается нередко. Что, в свою очередь, ведет к вышеописанным ситуациям несанкционированных послаблений. И в таких случаях собственные сотрудники становятся главной угрозой многим внутренним корпоративным сетям.

На самом деле, все не так уж и грустно. И в этой статье мы рассмотрим основные шаги, которые системный администратор или человек, отвечающий за ИТ-безопасность внутри компании, сможет сделать для проверки и улучшения общего состояния безопасности внутренней сети. Основное внимание будет уделено банальным, но в то же самое время, с точки зрения аудитора, весьма критическим вещам.

Пароли

Доминирующая практика, особенно в небольших компаниях, — один пароль навсегда, причем достаточно легкий для запоминания. Не стоит объяснять, что такая практика порочна. И с увеличением количества пользователей сети шансы того, что один из них «засветит» свой пароль, увеличиваются. Да и простой пароль легко взломать атакой по словарю или перебором. Для этого и существуют программные методы запроса юзера на смену пароля, проверки на повторяемость и криптографическую сложность. С введением сложных, часто меняемых паролей возникает новая проблема: их начинают забывать или ставить один и тот же пароль во множестве различных мест, включая Интернет-ресурсы. Но кто может поручиться за намерения владельца ресурса или за сохранность этих данных вне компании? Что если сессия к такому удаленному ресурсу перехвачена злоумышленником с помощью атаки «человек в середине»? Что если один из маршрутизаторов на пути к ресурсу взломан и используется для отзеркаливания проходящего через него трафика на хост с установленным сниффером? Практика ограничения доступа к внешним ресурсам распространена, но что можно сделать, если логины на внешних ресурсах необходимы для работы? Остается донести до каждого сотрудника через политику безопасности то, что внешние и внутренние пароли совпадать не должны. К сожалению, часто сами системные администраторы задают один и тот же пароль для всех серверов и/или сетевых устройств, что недопустимо. Встречаются случаи, когда пароль для входа на коммутаторы совпадал с паролем для их мониторинга SNMP-сообществом или же пароль для входа на мобильный хост совпадал с WPA-PSK-ключом для подсоединения к беспроводной сети. Последнее наиболее характерно при использовании Windows-настроек EAP-PEAP по умолчанию. Это безусловно удобно для работы, но с точки зрения сетевой безопасности таких вещей желательно избегать.

Вне зависимости от сложности внедренной политики и частой смены паролей, пытливый ум ленивого пользователя всегда найдет способ облегчить свою жизнь. Чаще всего он записывает пароли на бумажках, приклеивает их к монитору или «прячет» под клавиатурой. Найдя такого рода информацию, аудитор сразу же получает, как минимум, пользовательский доступ к ресурсам сети. В практике были случаи, когда подобные шпаргалки были прикреплены не только к машинам простых пользователей, но и находились на различных сетевых устройствах, включая межсетевые экраны, серверы, коммутаторы и пр. Бороться с подобной практикой достаточно легко: пара показательных наказаний — и пользователи начнут тренировать мозг на запоминание или по крайней мере прятать шпаргалки как следует. Но для того чтобы с этим бороться, все до единого сотрудника должны быть ознакомлены с политикой применения безопасных паролей и наказаниями за ее нарушение. Ознакомившись, они обязаны ее подписать. В ряде компаний подобные вещи справедливо включают в контракт, подписываемый при приеме на работу. И аудитор помимо проверки силы паролей безопасности хранения и частоты их смены должен также убедиться в том, что:

1. использование безопасных паролей детально описано в политике безопасности и других аналогичных документах;
2. то, что принято в компании на практике, полностью совпадает с вышеобозначенной документацией;
3. все сотрудники ознакомлены с правилами составления и применения паролей;
4. подписанные всеми правила хранятся в надежном месте на случай административного или юридического разбирательства.

Токены, смарткарты и мобильные телефоны

Огромное количество проблем, связанных с безопасностью паролей, решаются путем внедрения токенов для двухфакторной аутентификации, которые предлагают такие производители, как RSA, Passlogix, Аладин и др. Тем не менее не следует считать, что внедрение токенов или смарткарт раз и навсегда решит все проблемы аутентификации. Если построить шкалу между уровнем безопасности и легкостью внедрения и управления системой аутентификации, то пароли окажутся на одном ее конце, токены и смарткарты — на противоположном. В то время как при правильном обращении токены очень безопасны, пользователи имеют тенденцию их регулярно терять или, по крайней мере, оставлять без присмотра. Проводя аудит, проверьте, не валяются ли токены или смарткарты на столах сотрудников и их легко можно выкрасть. Особенно такие ситуации часты, когда одному и тому же человеку необходимо иметь множество токенов для доступа на различные ресурсы, к примеру принадлежащие удаленным отделам или партнерским компаниям.

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD, И КОНСТАНТИН ГАВРИЛЕНКО, MD ARHONT LTD

В настоящее время активно развивается компромиссный метод, основанный на применении мобильных телефонов вместо токенов, с пин-кодом, присылаемым по запросу на аутентификацию через SMS. В зависимости от изначальных установок такой логин-код может быть использован как однократно, так и несколько раз, а также на протяжении обозначенного периода времени (скажем, в течении трех часов). Это позволяет хранить на одном мобильнике логин на множественные ресурсы, кроме того, пользователи склонны более тщательно следить за своими телефонами, чем за дешевыми корпоративными токенами, и меньше их терять. Тем не менее и здесь есть свои проблемы. Проводя аудит и зная, что в компании принята подобная система, проверьте, не оставляют ли эти телефоны без присмотра и не одалживают ли их коллегам, друзьям и т. д. Также рекомендуется быстрое сканирование на предмет их открытости через Bluetooth и наличия распространенных уязвимостей, позволяющих «вытянуть» из телефона полученные сообщения (вместе со всеми присланными пин-кодами, которые на момент атаки могут быть действительными). А смартфоны с возможностью подключения к рабочим станциям и даже локальным сетям, например через Wi-Fi, и используемые для двухфакторной аутентификации не должны к ним быть подключены постоянно, если такое подключение вообще разрешается политикой безопасности компании. В любом случае, используются ли в качестве замены паролям токены, выходящие из моды смарткарты или же мобильники, контроль за этими устройствами должен быть жестким, включая детальную инвентаризацию, отчетность и адекватную реакцию на потерю или похищение таких устройств. И при проведении внутренних аудитов все эти меры должны быть тщательно проверены — и на бумаге, и на практике.

Незащищенные системы

Как правило, большинство сотрудников компании, покидая свое рабочее место, не удосуживаются выйти из системы или временно закрыть доступ к компьютеру, тем самым предоставляя злоумышленнику право делать что угодно от лица этого пользователя. Системному администратору, в первую очередь, следует попытаться донести до каждого, что он несет всю ответственность за действия, произведенные с его аккаунта и системы. На самом деле достаточно легко установить своевременное отключение доступа через заданное время после определенного периода неактивности, используя встроенные методы хранителя экрана или операционной системы. При этом стандартной практикой является блокирование аккаунта после трех неуспешных попыток доступа для предотвращения попыток угадать пароль. Кажется мелочь,но отсутствие такой мелочи может в два счета привести к получению отрицательного заключения от аудитора.

Если доступ к компьютеру закрыт экраном логина, атакующий может всегда перегрузить хост с дискеты, CD или флэшки для смены пароля. Также помните, что для станций, на которых установлены множественные операционные системы, уровень безопасности при перезагрузке равен уровню для самой незащищенной системы. В классическом варианте Windows/Linux если одна из систем не запаролена в бутлоадере, то защита другой системы бутлоадер-паролем более не имеет значения — получить доступ из одной системы к другой на одном хосте элементарно. Посему, если не все, то хотя бы критические системы, хранящие конфиденциальную информацию, должны быть защищены BIOS-паролями, а методы загрузки с периферических устройств должны идти в BIOS-списке только после загрузки с жесткого диска. Защищать паролем бутлоадера полезно, но далеко не так надежно, как в случае защиты BIOS'a.

Для того чтобы выдать конфиденциальную информацию посторонним, необязательно отходить от своей рабочей станции. В английской ИТ-терминологии есть даже специальный термин для обозначения подглядывания на экран через плечо — «shoulder surfing». В первую очередь, все вводимые пароли на экране монитора должны обозначаться звездочками, причем количество звездочек не должно совпадать с количеством символов в пароле. В большинстве операционных систем при логине так оно и есть, тем не менее доводилось видеть коммерческие приложения, в том числе разработанные внутри клиентских компаний, где эта элементарная мера безопасности отсутствует напрочь. Пользователи должны быть предупреждены о «сующих свой нос через плечо» без надобности и реакции на такие инциденты. Все эти моменты должны быть отражены в политике безопасности, которую, как и полагается, все пользователи обязаны изучить и подписать.

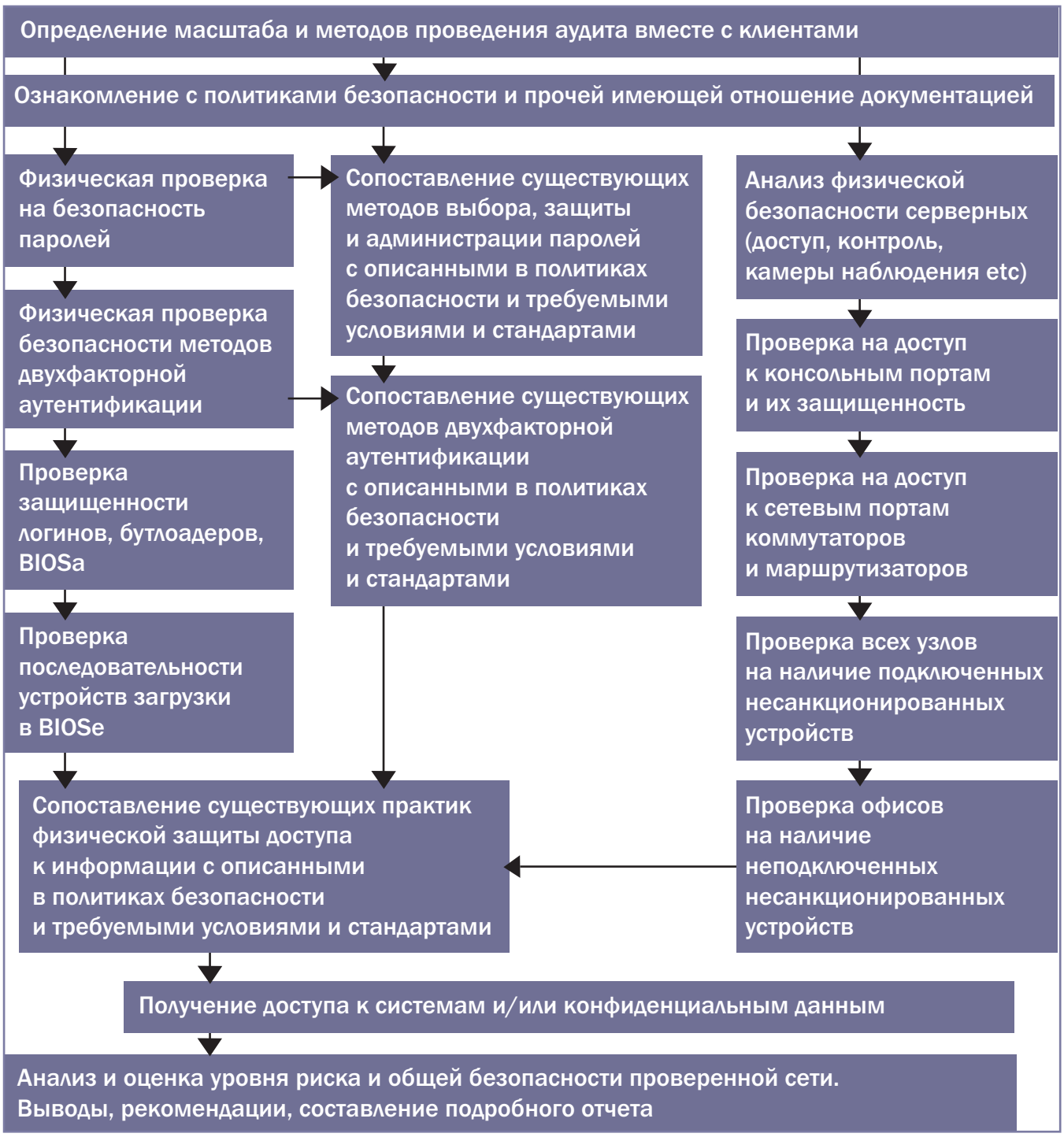
Порты хостов, коммутаторов и беспроводные устройства

Во многих компаниях и организациях запрещено подключение физических носителей памяти к портам корпоративных систем. Проводя аудит, проверьте, так ли это. Убедившись, что так, осмотрите рабочие станции и серверы на предмет подсоединенных устройств. Одновременно убедитесь, что подобного рода устройства не валяются на столах у сотрудников и т. д. По чеховской схеме, если на стене висит ружье, то оно рано или поздно стреляет. Точно так же если на столе или еще где лежит флэшка или Zip диск, то рано или поздно его подключат, а скорее всего уже подключали — не для красоты он там лежит. Медиаплейеры и цифровые фотоаппараты должны также внушать подозрения — в конечном итоге это те же физические носители памяти, которые можно использовать для чего угодно, помимо музыки и фотографий. Осмотрите порты на предмет наличия подключенных неизвестных устройств, к примеру физических кейлоггеров типа PS/2-to-PS/2. С помощью таких бесхитростных устройств с памятью в 64 Кбайта, установленных внутренними мошенниками в лондонских офисах, всемирно известный японский банк «Сумитомо» чуть было не потерял 400 млн. долл. Деньги удалось вернуть, но репутация банка оказалась подмоченной. В то же время существуют централизованные коммерческие решения, позволяющие полностью блокировать (а если надо, и открывать) USB- и даже COM-порты защищаемых систем от подсоединения любых устройств.

Особое внимание уделяйте обнаружению несанкционированных беспроводных устройств любого типа — от точек доступа до миниатюрных клиентских USB-устройств, как для 802.11, так и для Bluetooth. Такие устройства открывают прямую возможность наружного доступа к вовлеченным системам и внутренним сетям компании, минуя все меры защиты периметра этих сетей. Ни одна здравомыслящая компания не должна разрешать сотрудникам приносить и подключать любые беспроводные устройства на ее территории, как бы им не было удобно их использовать. А если мобильные компьютеры сотрудников компании поддерживают беспроводную связь (а это относится ко всем современным ноутбукам и наладонникам), но при этом беспроводной сети в компании нет, то системные администраторы обязаны позаботиться о том, чтобы драйверы для клиентских беспроводных устройств этих компьютеров были удалены и работать они никак не могли. Если пользователь собственноручно установит драйверы и включит устройство, то это безусловное нарушение корпоративной политики безопасности, которое должно наказываться как минимум изъятием мобильного компьютера и выговором. При наличии же беспроводной сети системные администраторы должны озаботиться не только стандартными (соглас-

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD, И КОНСТАНТИН ГАВРИЛЕНКО, MD ARHONT LTD

ОБЩАЯ СХЕМА ПРОВЕДЕНИЯ ВНУТРЕННЕГО ФИЗИЧЕСКОГО АУДИТА ИТ-БЕЗОПАСНОСТИ



АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD, И КОНСТАНТИН ГАВРИЛЕНКО, MD ARHONT LTD

но 802.11i стандарту) методами их защиты, но и регулярной чисткой Windows-профилей, содержащих информацию о подключаемых беспроводных сетях, а также регулярными обновлениями драйверов беспроводных устройств во избежание атак. И аудиторы должны тщательно все эти вещи проверить и в плане политики безопасности и наличия всей документации, и в плане соблюдения вышеуказанных мер на практике.

В заключение стоит упомянуть порты корпоративных коммутаторов. Все неиспользуемые порты коммутаторов должны быть отключены напрочь. При этом не мешает поместить их на отдельную виртуальную локальную сеть (VLAN), не имеющую никаких маршрутов. Что же касается портов, к которым подключены рабочие станции пользователей, то они все должны быть настроены как порты доступа без возможности манипуляции для превращения их в стволовые. На коммутаторах Cisco простая команда switchport mode access на каждом из таких портов может спасти компанию от крупных неприятностей. Кроме того, необходимо защитить эти порты от несанкционированной инъекции STP-фреймов (сочетание функций portfast и portguard в случае с коммутаторами Cisco и т. д.). Впрочем, это уже тема отдельного разговора…

Заключение

Нередко встречаются ситуации, когда при наличии самых современных, корректно и тщательно отлаженных средств защиты систем и сетей, таких как распределенные проводные и беспроводные системы предотвращения несанкционированного доступа, достаточно заурядными мерами обеспечения информационной безопасности просто пренебрегают. Часто это происходит из-за смещения баланса между безопасностью и удобством применения в сторону последнего, особенно под давлением пользователей среди руководящего состава. И неприятные инциденты, произошедшие в таких условиях, вдвойне обидны. Поэтому построение системы информационной безопасности компании или организации и проверку ее функциональности и полноценности всегда следует начинать именно с обыденных и внешне неприглядных вещей. **it**

Активный аудит

Существующие подходы к проведению аудита информационной безопасности (ИБ) обладают серьезными недостатками, прежде всего неполнотой и неадекватностью получаемых результатов. И по мнению Михаила Маркевича, аналитика по информационной безопасности, наиболее оптимальным является идея активного аудита. Активный аудит сочетает тест на проникновение и аудит ИБ в традиционном понимании. В основе активного аудита лежат несколько основополагающих принципов.

1. Наличие четкого описания модели нарушителя, в рамках которой действуют аудиторы. Рассматриваются отдельно внутренний нарушитель (например, сотрудник компании) и внешний нарушитель (хакер, действующий через Интернет). Уровень квалификации нарушителя считается достаточным для выполнения сложных задач по проникновению в информационную систему. Это автоматически означает, что квалификация самих аудиторов должна соответствовать данному уровню.

2. Уточнение области проведения аудита непосредственно в процессе работы на объекте. На практике заказчик часто предоставляет ограниченный набор сведений об информационной системе (что происходит, когда информационная система развивалась непланомерно и, как следствие, плохо документировалась), а аудиторы проводят инвентаризацию ресурсов информационной системы. Это позволяет выявить «потерянные» ресурсы (и в большинстве случаев плохо защищенные), что особенно актуально для крупных корпоративных информационных систем.

3. Аудитор изначально имеет только физический доступ к обследуемой информационной системе, логические права доступа (аутентификационные данные) ему не предоставляются (за редким исключением). Далее аудитор отрабатывает все возможные пути повышения привилегий от «нулевого» уровня, оценивая критичность и вероятность их реализации.

4. С одной стороны, например, наличие уязвимости в программном обеспечении автоматически не приводит к нарушению безопасности, так как многие уязвимости могут быть успешно реализованы только при определенном сочетании факторов. С другой стороны, использование штатных функций (именно функций, а не ошибок программного обеспечения или конфигурации) информационной системы в определенной комбинации может привести к нарушению ИБ. Выявление таких ситуаций невозможно без применения творческого, неформального подхода к анализу защищенности, хотя сами пути повышения привилегий, безусловно, легко формализовать и зафиксировать документально.

5. Анализ влияния выявленных в ходе активного аудита уязвимостей на защищенность всей информационной системы в целом. Критика существующих подходов аудита ИБ, в частности, заключается в том, что выявленные в ходе аудита уязвимости «всего лишь» отражают состояние информационной системы на момент аудита. Предлагаемый подход, который ставит своей целью сделать аудит более эффективным и актуальным, заключается в следующем: не столь важно, какая именно уязвимость была обнаружена, важно то, как наличие той или иной уязвимости влияет на защищенность всей информационной системы, насколько вся система устойчива к уязвимостям. Другими словами, в ходе аудита проводится анализ архитектуры безопасности информационной системы.

6. Поиск новых уязвимостей (не зафиксированных в различных базах уязвимостей, таких как CVE, OSVDB и т. п.) непосредственно в ходе работы на объекте в режиме реального времени.

7. Строгая система классификации уязвимостей. Каждая выявленная в ходе аудита уязвимость оценивается (по шкале с простыми и понятными описаниями уровней) с точки зрения ее критичности, простоты и вероятности реализации. Эти данные в дальнейшем используются для проведения анализа информационных рисков.

8. Отказ от приоритетного использования сканеров уязвимостей. Подобный инструментарий используется только на этапе предварительного сбора информации для автоматизации рутинной работы. Существенным недостатком сканеров является большое количество ложных срабатываний и невозможность обнаружения уязвимостей, отсутствующих в базе сканера (например, недавно появившихся уязвимостей, большого числа локальных уязвимостей, нетривиальных ошибок конфигурации).

9. Применение методов социальной инженерии для имитации действий нарушителя ИБ, направленных на пользователей информационной системы компании. Эти методы позволяют оценить уровень квалификации пользователей в области обеспечения ИБ и вероятность реализации атак, выполняемых нетехническими способами.

По материалам Digital Security (www.dsec.ru/about/articles/active_audit/)