

Аудит сети

Анализ защищенности сетевых ресурсов

Аудит сети позволит увидеть текущее состояние сетевых ресурсов, проанализировать его и вывести заключение о состоянии защищенности сети. Предложения по изменению настроек сетевых ресурсов и других соответствующих действий позволят поднять уровень Информационной безопасности организации.

Также будет получена «Карта сети» – некий «слепок» текущего состояния, что в последующем позволит анализировать происходящие изменения в сети. Это может быть полезно как для плановой проверки состояния ресурсов, так и для анализа возможных форс-мажорных событий.

Кратко об Аудите сети и Анализе защищенности

Известно, что компьютерным преступником может быть любой. Типичным компьютерным преступником принято представлять немолодого хакера, использующего телефон и домашний компьютер для получения доступа к информационным ресурсам. Но наиболее опасный компьютерный преступник - это служащий, которому разрешен доступ к системе, пользователем которой он является. По разным оценкам экспертов до 90% информации теряется в результате умышленных или безответственных действий сотрудников организации.

Аудит состоит в оценке текущего состояния информационной безопасности в Информационной системе (ИС). Также он проводится при оценке на соответствие предъявляемым требованиям и стандартам по вопросам информационной безопасности: действующего законодательства, нормативных и регламентирующих документов и т.д.

Целесообразность проведения аудита:

- перед проектированием некоторой системы Обеспечения Информационной безопасности (ИБ);
- после создания такой системы для оценки степени выполнения требований, сформированных на этапе проектирования;
- периодически - например, один раз в полгода - для оценки текущего состояния информационной безопасности. Поскольку любая система со временем развивается и изменяется, что сказывается на уровне защищенности информации.

В ходе проведения информационного аудита наши эксперты по формальным критериям оценивают степень соответствия компонентов и процессов ИС на соответствие требованиям по безопасности информации.

Цель аудита сети - анализ уязвимостей компонентов автоматизированных систем в организации таких как: сервера баз данных, межсетевые экраны, маршрутизаторы, рабочие станции и т.д.

Поиск уязвимостей производится с помощью средств автоматического сканирования, а результаты оцениваются нашими экспертами.

Работы по исследованию сети

Комплекс работ по исследованию защищенности информационной системы включает в себя:

1. Поиск информации, касающейся клиента и сотрудников клиента в сети Интернет;
2. Внешний аудит (тестирование на проникновение);
3. Внутренний аудит (сканирование ЛВС заказчика);
4. Плановый Аудит Сети. Аутсорсинг по вопросам Информационной безопасности
5. Предоставление отчета по выявленным уязвимостям с приоритетом по степеням угроз;
6. Рекомендации по устранению существующих уязвимостей;

1. Этап «Поиск информации, касающейся клиента и сотрудников клиента в сети Интернет» включает в себя:

- структурирование найденной в Интернет информации о Компании;
- проведение специализированного поиска информационных взаимосвязей между событиями, людьми, адресами и т.п.;
- проведение анализа результатов поиска и выявления явных или скрытых угроз для функционирования предприятия Заказчика.

2. Внешний аудит (тестирование на проникновение из Интернет).

Данный комплекс работ включает в себя выявление в предоставленных для исследования Интернет-ресурсах Заказчика уязвимостей и определение их уровня опасности, а также тестирование на проникновение.

Целью теста на проникновение является проверка наличия слабых мест или уязвимостей в защите Вашего веб-сервера корпоративной сети "извне", а также используемых интернет-приложений.

В рамках внешнего аудита проводятся:

- Проверка на возможность проникновения в локальную сеть компании, похищения и порчи данных;
- Обследование возможных угроз (в том числе электронной почты, систем обмена сообщениями ICQ и др.);
- Проверка файрволла на неуязвимость со стороны Интернет;
- Обследование Web и Почтового серверов (в случае наличия).

В случае обнаружения уязвимостей, Исполнитель предоставляет документальные доказательства возможности компрометации, искажения, уничтожения критичной информации Заказчика в предоставленных для исследования Интернет-ресурсах Заказчика.

3. Внутренний аудит (сканирование ЛВС заказчика внутри сети).

Некоторые из этапов

- Проверка настроек политики безопасности на серверах;
- Проверка файрволла на неязвимость из разных сегментов сети;
- Обследование всех рабочих станций в офисе на предмет соблюдения правил информационной безопасности. Выявление незарегистрированных модемов, несанкционированных средств сокрытия информации и прочее;
- Проверка возможности перехвата сетевых пакетов в локальной сети;
- Проверка баз данных (бухгалтерских БД: DBF, Инфин; почтовых БД: MS Exchange, Lotus, Domino) на возможность получения неавторизованного доступа с различных рабочих мест компании;
- Проверка эффективности работы антивирусной системы.

Сканирование позволяет выявить уязвимости, которые есть в сети, дает четкую картину того, что видит взломщик при атаке на компьютеры или сеть.

Результатом прохождения теста станет отчет (экспертное заключение), который предоставит Вам истинную картину о состоянии защиты вашей системы от НСД на текущий момент времени. Отчет подтвердит или опровергнет возможность несанкционированного доступа к защищаемым ресурсам информационной системы.

В процессе тестирования будет установлено:

- какую информацию о вашей ИС можно получить в Интернет;
- каким образом реагирует защита Вашей сети на имитацию атаки извне;
- возможен ли взлом ИС, используя открытую информацию о вашей ИС;
- размер потенциальных потерь в случае инцидента (взлома).

В случае обнаружения каких-либо упущений будут даны практические рецепты их устранения, а в случае наличия реальных или потенциальных угроз Вашим информационным ресурсам, будут даны советы по улучшению их защиты.

Любой узел, предоставляющий какой-нибудь сервис, не может быть на 100% защищен. Если компьютер уязвим, то уязвимость в какой-то момент времени может быть использована. Даже наиболее сложные системы безопасности могут иметь "дыры" и аудит системы безопасности с внешней стороны является наилучшим способом обнаружить это.

Сканирование включает более 1000 тестов для ОС UNIX, Windows и активного сетевого оборудования. Некоторые тесты называются "сбор информации" и проводятся для того, чтобы показать, что постороннее лицо может узнать о вашем компьютере. Остальные тесты проверяют уязвимость систем, путем сканирования на наличие известных "дыр". Каждый компьютер сканируется на наличие открытых портов и запущенных сервисов.

Сканирование не наносит вреда, так как "разрушительные" действия не предпринимаются. Риск минимизируется, избегается перегрузка сети или превышение максимума пропускной способности.

Эти работы ни в коем случае не заменяют полного комплекса мер по обеспечению режима безопасности. Они всего лишь помогают быстро проверить сотни узлов, в т.ч. и находящихся на других территориях. Они помогут обнаружить практически все известные уязвимости и порекомендовать меры по их устранению. Надо помнить, что инструментальное сканирование это всего лишь часть эффективной политики безопасности сети, которая складывается не только из применения различных технических мер защиты (средств анализа защищенности, систем обна-

ружения атак, межсетевых экранов и т.п.), но и из применения различных организационных и законодательных мер.

«Карта» сети

Точная и надежная фиксация информации о компонентах корпоративной сети и данных, с момента их создания или появления до момента их уничтожения, является залогом успешного обнаружения практически любых нарушений безопасности. Такие данные позволят сравнивать эталонную информацию о состоянии информационной системы при ее создании (или в момент последнего санкционированного изменения) с текущим состоянием и своевременно обнаруживать все несанкционированные изменения.

Подходы к обнаружению таких изменений обычно основаны на определении различий между текущим состоянием контролируемого объекта и предварительно зафиксированным, ожидаемым состоянием. Персоналу защиты необходимо всегда знать, где и какой ресурс находится, а также состояние этого ресурса. Без этой информации нельзя адекватно определить было ли что-нибудь добавлено, изменено, нарушено и т.д. Особенно это важно во многих российских компаниях, в которых всегда присутствуют "продвинутые" сотрудники, которые, считая себя компетентными во всем, самостоятельно реконфигурируют свои рабочие станции и сервера, не ставя в известность IT-персонал. Хорошо еще, если это рядовой сотрудник, который не может сделать ничего за пределами своего компьютера. А если это администратор, который на свой страх и риск изменяет конфигурацию своего сегмента сети?

Однако, стоит отметить, что данным этапом, который называется «построение карты сети», обычно пренебрегают во многих организациях. Это связано с тем, что процесс фиксации необходимого объема информации о компонентах информационной системы - достаточно долгий и рутинный процесс, который требует не только материальной поддержки. Зачастую специалисты отделов защиты информации не имеют соответствующей подготовки для получения такой информации. Мало того, они не имеют и доступа к оборудованию, функционирующему в сети.

Как показывает российская практика, карта сети создается (если вообще создается) только на этапе проектирования информационной системы. Затем эта карта уже не поддерживается в актуальном состоянии и не может служить основой для контроля и обнаружения несанкционированных изменений.

Кроме того, зачастую данная «карта» сети находится только в управлениях информатизации (отделах ИТ) и является недоступной для отделов ИБ, что существенно снижает эффективность их работы.

Обнаружение конфигураций "по умолчанию".

Как показывает практика, многие системные администраторы устанавливают операционные системы, прикладное программное и сетевое программно-аппаратное обеспечение в конфигурации, заданные "по умолчанию". С одной стороны, это существенно облегчает и ускоряет им работу, а с другой - приводит к тому, что злоумышленники, используя известные слабости таких конфигураций, проникают на узлы корпоративной сети. Системы анализа защищенности могут быть настроены на поиск узлов с программным обеспечением, установленным в конфигурации "по умолчанию", и рекомендовать шаги по устранению найденных проблем.

Обнаружение модемов.

Очень часто сотрудники компаний, в которых доступ в Internet регламентируется и разграничивается с помощью различных защитных средств (например, межсетевых экранов или систем контроля содержания), подключают к своим компьютерам модемы и используют их для выхода в Internet в обход защитных механизмов. Также модемы очень часто используются для получения обновлений различных юридических и бухгалтерских программ (например, Консультант-Плюс или 1С:Бухгалтерия). И, наконец, модемы могут быть использованы для доступа к рабо-

чему месту из дома. Это представляет большую угрозу для многих компаний, т.к. компьютеры, к которым подключены модемы, никак не защищены и любой злоумышленник, обнаруживший такой "черный ход", может воспользоваться им для несанкционированного доступа к ресурсам, требующим обязательной защиты. Некоторые системы анализа защищенности позволяют своевременно обнаружить в корпоративной сети модемы и указать на их наличие администратору безопасности.

Обнаружение неизвестных устройств.

Нередки случаи, когда злоумышленники подключают свои компьютеры или notebook'и к критичным сегментам сети с целью получения доступа к передаваемой конфиденциальной информации (например, паролям или платежным поручениям). Установленные на таких компьютерах анализаторы протоколов (снифферы) позволяют перехватывать весь сетевой трафик, циркулирующий между узлами критичного сегмента. Опасность таких несанкционированно подключенных устройств в том, что они без труда получают доступ к паролям пользователей (в т.ч. и администратора), передаваемых в незащищенном виде по большинству протоколов, построенных на базе стека TCP/IP. В частности беззащитными к чужому любопытству являются протоколы: HTTP, FTP, Telnet, POP3, IMAP и т.д. В том числе открытой остается и информация, передаваемая между SQL-сервером и клиентским программным обеспечением.

Системы анализа защищенности позволяют своевременно обнаруживать в корпоративной сети несанкционированно подключенные устройства и оповещать об этом администратора безопасности.

4. Плановый Аудит Сети. Аутсорсинг по вопросам Информационной безопасности

Такие работы позволят поддерживать степень защищенности сетевых ресурсов на необходимом Заказчику уровне и оперативно реагировать на возможные внештатные ситуации. Также, с помощью этого эффективного инструмента, специалисты по ИБ в организации смогут осуществлять необходимый им контроль за функционированием сети и работой IT отдела.

Объемы планового аудита и целесообразные сроки его проведения будут видны после проведения работ по первому Аудиту сети. Исходя из этого, будет рассчитываться и сумма за услуги.

Вполне возможно, что необходимость в отслеживании изменений сетевых ресурсов будет распространяться только на критически важные объекты, а не на всю сеть. Например, сервер Базы Данных, Межсетевой Экран, рабочие станции менеджмента или бухгалтерии. Вариант, когда планомерно исследуются только сегменты, а не вся сеть, позволит сэкономить компании затраты на безопасность.

Учитывая, что в каких-то вопросах специалист по ИБ организации будет нуждаться в помощи, мы готовы оказывать такие консультации и оперативно решать возможные вопросы и форс-мажорные ситуации, возникающие в процессе работы компании. Необходимые объемы, способ реагирования и другие вопросы обсуждаются в ходе выполнения работ.

5. Результаты Аудита и Анализа. Отчет

Предоставление отчета по выявленным уязвимостям с приоритетом по степеням угроз.

В результате проведения обследования Заказчик получает:

- перечень выявленных уязвимостей (слабых мест) в настройках оборудования, сетевых сервисов, операционных систем и прикладного программного обеспечения;
- подробное описание каждой обнаруженной уязвимости, ее расположение и оценку возможных последствий ее использования злоумышленниками.

6. Рекомендации по устранению существующих уязвимостей.

После внутреннего и внешнего обследования предоставляются рекомендации по устранению существующих уязвимостей, а также возможных потенциальных угроз:

- рекомендации по нейтрализации уязвимостей (снижению возможного ущерба от их использования злоумышленниками);
- рекомендации по изменению конфигурации и настроек компонентов АС, используемых защитных механизмов;
- рекомендации по установке необходимых обновлений (patches, hot-fixes) установленно-го программного обеспечения;
- рекомендации по изменению политик безопасности на Серверах и Рабочих станциях;
- в ПО - Lotus Domino, Ms Exchange (в случае наличия);
- в настройках файрволла;
- в Антивирусной системе;
- в Бухгалтерских Базах Данных;
- и т.п.

Рекомендации включают в себя подробные пошаговые инструкции для устранения уязвимостей, предназначенные как для системного администратора, так и для пользователей.

На основании результатов проведенных работ Заказчик сможет:

- Определить эффективность защиты критичной информации от несанкционированного доступа через Интернет;
- Устранить существующие уязвимости в принадлежащих Заказчику Интернет-ресурсах;
- Уменьшить риск несанкционированной компрометации, искажения, уничтожения критичной информации Заказчика со стороны глобальной компьютерной сети Интернет.

Технология сканирования сети не является скрываемой нашими специалистами. Сотрудники IT отдела организации смогут наблюдать за работой нашего специалиста, что, возможно, не будет лишним в плане их эрудиции и знаний. В процессе такого сотрудничества возможные явные ошибки в настройках устройств сети, политик доступа к ресурсам и т.п. могут исправляться специалистами компании сразу же, не ожидая получения результатов работ в оформленном виде.