Аудит информационной безопасности — независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций. Аудит ИБ позволяет получить наиболее полную и объективную оценку защищенности информационной системы (ИС), локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения ИБ организации. В рамках аудита ИБ или отдельным проектом может быть проведен тест на проникновение, позволяющий проверить способность ИС компании противостоять попыткам проникновения в сеть и неправомочного воздействия на информацию.

Аудит безопасности сайта

аудит безопасности сайта, проверка сайта на уязвимости

Комплексный аудит безопасности веб-приложения

Аудит безопасности сайта на наличие уязвимостей является мощным инструментом для обеспечения информационной безопасности ресурса. Аудит сайта на наличие уязвимостей — это комплекс работ по выявлению ошибок в коде сайта и программном обеспечении сервера, воспользовавшимися которыми злоумышленники могут атаковать и взломать сайт. Как правило, в эти работы входят такие мероприятия как: сканирование сайта на уязвимости, ручной анализ содержимого сайта, поиск и выявление ошибок в логике работы скриптов и компонентов веб-приложения.

Зачастую, к аудиту безопасности сайта прибегают постфактум, уже после того как сайт был взломан, отмечен в поисковой выдаче как вредоносный и удален со своих позиций. Трафик на сайт падает до минимальных значений, клиенты и сотрудники оповещают о том, сайт заражен вирусами. Чтобы избежать взлома сайта злоумышленниками необходимо проводить регулярный аудит безопасности и строго следовать рекомендациям специалистов.

Проверка сайта на уязвимости будет осуществляться путем тестирования на устойчивость к комбинированным методам атак и основана на методологиях **OWASP, WASC, OSSTMM**, а также лучших практиках и рекомендациях стандарта PCI DSS. Все работы подкрепляются обширным практическим опытом наших сертифицированных специалистов. В случаях, когда

сайт создан на основе популярной CMS (Битрикс, NetCat, WordPress, Joomla!, Drupal и многие другие), дополнительно будет проведена проверка устойчивости системы к известным эксплоитам. Для предотвращения взлома сайта на популярных CMS мало устанавливать последние обновления. Необходимо удалять старые учетные записи, проверять актуальность плагинов, расширений и модулей, обращать внимание на служебные скрипты и настройку хостинга - весь комплекс таких услуг и представляет собой аудит безопасности сайта. По результатам проверки сайта на уязвимости, заказчик услуги получает отчет и рекомендации по исправлению обнаруженных уязвимостей. Все работы ведутся строго по договору и согласшения о неразглашении (NDA).

Ежеквартальный аудит безопасности сайта в автоматическом режиме

Аудит безопасности в автоматическом режиме способен обнаружить до 70% распространенных уязвимостей. Такой аудит позволяет владельцам сайта своевременно получать информацию об уязвимых и потенциально уязвимых веб-сервисах, и, обладая такой информацией, вовремя их устранять. Аудит безопасности в автоматическом режиме (тариф "АВТО") позволяет обнаружить большинство уязвимостей, выявляемых популярными сканерами веб-приложений, которыми активно пользуются злоумышленники.

Тестирование на проникновение

тестирование blackbox (имитация действий злоумышленника) и whitebox (анализ исходного кода)

Тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) является популярной во всем мире услугой в области информационной безопасности. Суть таких работ заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор играет роль злоумышленника, мотивированного на нарушение информационной безопасности сети заказчика.

Как правило, интенсивной проверке подвергаются технические средства защиты корпоративной сети, но в зависимости от поставленных условий, могут оцениваться и другие аспекты безопасности, например — уровень осведомленности пользователей.

Процесс тестирования на проникновение подразумевает моделирование реальных действий злоумышленника – поиск уязвимостей системы защиты и их последующую эксплуатацию. Тест на проникновение позволяет получить независимую оценку и экспертное заключение о состоянии защищенности конфиденциальной информации.

По результатам работы нами готовится детальный отчет, который позволит Вам не только узнать о степени защищенности конфиденциальных данных, но и получить конкретные рекомендации по устранению выявленных угроз информационной безопасности.

Тест на проникновение поможет Вам избежать инцидентов, которые могут подорвать репутацию Вашей организации и принести Вам существенные убытки.

В ходе теста на проникновение осуществляются попытки эксплуатации обнаруженных уязвимостей ИС (иными словами, попытки проникновения в ИС). В случае успешной реализации, такие попытки позволяют эффективно продемонстрировать возможность проникновения в ИС и выявить слабые места в обеспечении информационной безопасности. Что в свою очередь позволяет отделить критические проблемы безопасности, требующие непосредственного внимания, от тех, которые представляют меньшую угрозу.

Это позволит разумно выделять финансовые и материальные ресурсы на обеспечение

безопасности ИС именно на тех участках, на которых это требуется больше всего.

Бесплатный первичный аудит внешнего периметра в режиме Black Box. Для предварительной оценки угроз безопасности внешнего периметра корпоративной сети мы предоставляем бесплатный сервис первичного аудита, позволяющий владельцу ресурса получить информацию об уязвимых или потенциально уязвимых сервисах, а также информацию о возможных векторах атак. Услуга предоставляется для коммерческих ресурсов. Решение о проведении первичного аудита рассматривается индивидуально

Нагрузочное тестирование

тестирование работы ресурса при высоких нагрузках

Нагрузочное тестирование ("load-testing, стресс-тестирование") — необходимо для определения или сбора показателей производительности и времени отклика программно-технической системы или устройства в ответ на внешний запрос с целью установления соответствия требованиям, предъявляемым к данной системе (устройству).

Для исследования времени отклика системы на высоких или пиковых нагрузках производится "стресс-тестирование", при котором создаваемая на систему нагрузка превышает нормальные сценарии её использования. Современная ИТ-инфраструктура должна обеспечивать необходимый уровень производительности. Любые сбои, задержки и отказы могут стать причиной потери клиентов, как текущих, так и потенциальных. Основная цель нагрузочного тестирования заключается в том, чтобы, создав определённую ожидаемую в системе нагрузку (например, посредством виртуальных пользователей), наблюдать за показателями производительности системы.