KASPERSKY lab

СЕРВИСЫ KASPERSKY SECURITY INTELLIGENCE

Экспертные сервисы

www.kaspersky.ru

ЭКСПЕРТНЫЕ СЕРВИСЫ

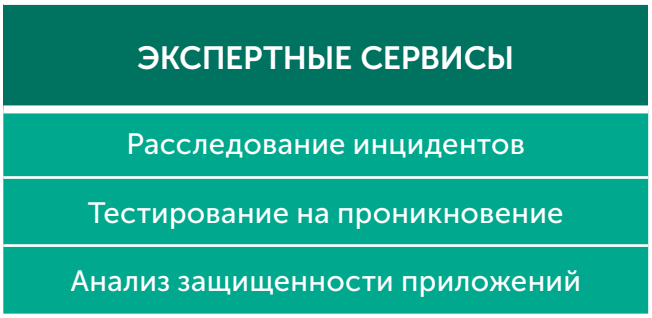
Экспертные сервисы «Лаборатории Касперского» – это услуги специалистов компании, многие из них являются признанными во всем мире профессионалами, знания и опыт которых служат опорой нашей репутации мирового лидера в области анализа угроз.

Каждая IT-инфраструктура уникальна, а самые опасные атаки специально разрабатываются с учетом уязвимостей конкретной организации. Поэтому и мы при оказании экспертных сервисов индивидуально подходим к каждому клиенту. На следующих страницах описаны сервисы, входящие в наш профессиональный пакет. Работая с вами, мы можем полностью или частично предоставлять их в любом сочетании.

«Лаборатория Касперского» стремится в первую очередь стать личным консультантом, который поможет вам оценить степень риска, усилить безопасность и уменьшить возможные последствия атак в будущем.

Предоставляемые экспертные сервисы:

- расследование инцидентов
- тестирование на проникновение
- анализ защищенности приложений



РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Цифровая криминалистика | Анализ вредоносного ПО

Индивидуальная помощь в расследовании инцидентов поможет вашей организации выявить и разрешить инциденты в сфере IT-безопасности.

Кибератаки становятся все более серьезной угрозой для сетей крупных предприятий. Злоумышленники подбирают эксплойты, использующие конкретные уязвимости в системе жертвы. Целью чаще всего становится кража или уничтожение конфиденциальной информации или объектов интеллектуальной собственности, остановка бизнес-процессов, повреждение промышленных систем или хищение денежных средств.

Защитить крупную компанию от таких изощренных, тщательно спланированных атак с каждым днем становится все сложнее. В некоторых случаях даже опытным IT-специалистам трудно определить, является ли их организация объектом атаки.

Сервис «Лаборатории Касперского» по расследованию инцидентов помогает компании-клиенту сформировать собственную стратегию защиты. Для этого мы тщательно проводим постинцидентный анализ и даем практические рекомендации по устранению каждого инцидента.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

Сервис «Лаборатории Касперского» по расследованию инцидентов помогает разрешить актуальные проблемы безопасности, узнать об особенностях поведения вредоносного ПО и последствиях заражения, а также получить практические рекомендации по восстановлению нормальной работы систем. Такой подход позволяет организациям:

- снижать затраты на решение проблем, связанных с заражением вредоносным ПО;
- предотвращать или останавливать возможную утечку конфиденциальной информации с зараженных устройств;
- снижать репутационные риски, связанные с нарушением нормальной работы организации в результате заражения;
- восстановить нормальную работу устройств, нарушенную в результате заражения.

Расследования в «Лаборатории Касперского» ведут опытные аналитики, имеющие большой практический опыт и знания в области цифровой криминалистики и анализа вредоносного ПО. По завершении расследования клиенту предоставляется подробный отчет с полной информацией о результатах расследования и предлагаемой программой действий для восстановления нормальной работы всех систем.

ЦИФРОВАЯ КРИМИНАЛИСТИКА

Цифровая криминалистика – это сервис, позволяющий клиентам с помощью экспертов «Лаборатории Касперского» получить более полное представление об инциденте. Если в ходе расследования инцидента было обнаружено вредоносное ПО, эксперты проведут его анализ. Чтобы воссоздать полную картину инцидента, специалисты «Лаборатории Касперского» анализируют различные исходные данные: образы жестких дисков, дампы памяти, трассировки сети и др.

Клиент начинает процесс расследования, собирая улики и предоставляя описание инцидента. Эксперты «Лаборатории Касперского» изучают особенности инцидента, в том числе идентифицируют исполняемые файлы вредоносных программ (если они есть) и проводят анализ вредоносного ПО. Клиенту предоставляется подробный отчет, содержащий в том числе меры, необходимые для устранения последствий инцидента.

АНАЛИЗ ВРЕДОНОСНОГО ПО

Анализ вредоносного ПО позволяет получить полное представление о поведении конкретных вредоносных программ, использованных в ходе атаки на вашу организацию, а также о целях, преследуемых злоумышленниками.

Эксперты «Лаборатории Касперского» осуществляют всесторонний анализ вредоносного образца, предоставленного вашей организацией, и составляют подробный отчет, в частности содержащий представленную ниже информацию.

- **Свойства образца**. Краткое описание и вердикт согласно классификации «Лаборатории Касперского».
- **Подробное описание вредоносного ПО**. Углубленный анализ функций, поведения и целей вредоносной программы, включая индикаторы заражения, а также вся информация, необходимая для нейтрализации угрозы.
- **Сценарий восстановления системы**. В отчете будут предложены шаги по устранению последствий заражения.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

Сервис «Лаборатории Касперского» по расследованию инцидентов может предоставляться:

- по подписке, предусматривающей расследование определенного числа инцидентов;
- как расследование единичного инцидента.

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Надежная защита IT-инфраструктуры от потенциальных кибератак – актуальная проблема в любой организации. Особенно сложной эта задача становится для крупных предприятий, где в подразделениях, разбросанных по всему земному шару, работают тысячи сотрудников и используются сотни информационных систем.

IT-специалисты и сотрудники отдела безопасности вашей организации упорно работают над тем, чтобы обеспечить защиту каждого компонента сети от злоумышленников, но при этом не затруднять доступ к ресурсам для своих пользователей. Однако киберпреступнику может оказаться достаточно одной-единственной неустраненной уязвимости, чтобы перехватить управление вашими информационными системами.

Тестирование на проникновение – это практическая демонстрация возможных сценариев атаки, позволяющих злоумышленнику обойти средства безопасности корпоративной сети, чтобы получить высокий уровень доступа к важным системам.

«Лаборатория Касперского» предоставляет сервис тестирования на проникновение, который позволит получить более полное представление о проблемных с точки зрения безопасности местах в инфраструктуре, выявить уязвимости, проанализировать возможные последствия атак различного вида и оценить эффективность уже принятых мер защиты, а также получить рекомендации по устранению уязвимостей и повышению безопасности.

Тестирование на проникновение, проводимое «Лабораторией Касперского», поможет вашей организации:

- выявить наиболее уязвимые места в сети,
- снизить риски, перераспределив ресурсы;
- избежать финансовых, операционных и репутационных потерь, вызванных кибератаками. Заблаговременное обнаружение и устранение уязвимостей сделает многие атаки просто невозможными;
- выполнить требования государственных, отраслевых или внутренних корпоративных стандартов, предусматривающих подобную форму оценки системы безопасности, например стандарта безопасности данных индустрии платежных карт (PCI DSS).

СОСТАВ РАБОТ И ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

В зависимости от задач и особенностей IT-инфраструктуры вы можете выбрать любые из следующих вариантов тестирования на проникновение.

- **Внешнее тестирование на проникновение**. Оценка системы безопасности, которая проводится со стороны сети интернет от лица злоумышленника, не обладающего никакими данными о вашей системе.
- **Внутреннее тестирование на проникновение**. Сценарии с участием злоумышленника, действующего внутри компании. Это может быть посетитель, у которого есть лишь физический доступ в помещения компании, или подрядчик, имеющий ограниченный доступ к системам.
- **Проверка уязвимости к социальной инженерии**. Оценка осведомленности персонала об угрозах безопасности. Моделируется применение методов социальной инженерии: фишинг, псевдовредоносные ссылки в сообщениях электронной почты, подозрительные вложения и т. д.
- **Оценка безопасности беспроводных сетей**. Наши эксперты выезжают к вам и проверяют состояние безопасности сетей Wi-Fi.

Тестирование на проникновение можно проводить в каком-то одном сегменте IT-инфраструктуры, однако мы настоятельно рекомендуем проверять таким образом всю сеть или хотя бы ее крупнейшие сегменты. Ведь результаты тестирования будут более достоверными, если наши специалисты смогут работать в тех же условиях, что и потенциальные злоумышленники.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Сервис тестирования на проникновение позволяет выявить бреши в системе безопасности, которыми злоумышленники могут воспользоваться для получения несанкционированного доступа к важным компонентам сети. Такими брешами могут выступать:

- уязвимая архитектура сети, ошибки конфигурации сетевого оборудования;
- уязвимости, делающие возможным перехват и перенаправление сетевого трафика;
- ошибки аутентификации и авторизации в различных службах;
- ненадежные пароли пользователей;
- недостатки конфигурации, в том числе предоставление пользователям слишком высоких полномочий;
- уязвимости, вызванные ошибками в коде приложений (внедрение операторов SQL, удаленное выполнение кода, загрузка произвольных файлов, межсайтовое выполнение сценариев и т. д.);
- уязвимости, вызванные использованием устаревших версий оборудования и программного обеспечения, для которых не были установлены последние обновления безопасности;
- разглашение информации.

По окончании работ у вас на руках окажется итоговый отчет с подробной технической информацией о ходе тестирования, его результатах и обнаруженных уязвимостях. В отчете также присутствуют рекомендации по устранению уязвимостей, наглядные иллюстрации направлений атак и выводы, резюмирующие результаты тестирования. В случае необходимости дополнительно могут быть подготовлены видеоматериалы и презентации для технических подразделений или для руководства.

ПОДХОД «ЛАБОРАТОРИИ КАСПЕРСКОГО» К ТЕСТИРОВАНИЯМ НА ПРОНИКНОВЕНИЕ

В рамках тестирования на проникновение имитируются настоящие кибератаки. При этом ситуация остается под полным контролем экспертов по безопасности «Лаборатории Касперского», которые уважают конфиденциальность ваших систем и не нарушают их целостность и доступность. Мы строго следуем международным стандартам и лучшим мировым практикам, в том числе:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Специалисты, проводящие работы, – опытные профессионалы, обладающие обширными и актуальными практическими знаниями. Наши эксперты известны своими исследованиями в области безопасности, в том числе обнаружением новых уязвимостей в крупнейших сервисах и программных продуктах, включая Oracle®, Google™, Apple®, Microsoft™, Facebook, Pay Pal, Siemens и SAP®.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

В зависимости от выбранного метода анализа защищенности, особенностей систем и бизнеса клиента сервис тестирования на проникновения может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно (так, внутреннее тестирование можно организовать через VPN-доступ), однако для оценки безопасности беспроводных сетей и ряда других задач необходимо присутствие специалистов на вашей территории.

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРИЛОЖЕНИЙ

Вы можете разрабатывать корпоративные приложения самостоятельно или приобретать их у сторонних поставщиков, но в любом случае даже одной ошибки в программном коде может быть достаточно, чтобы создать уязвимость для атак, которые приводят к значительным финансовым или репутационным потерям. Новые уязвимости могут также появиться в течение жизненного цикла приложения: в ходе обновления или из-за неправильной настройки компонентов. Кроме того, с течением времени появляются и новые способы атак, перед которыми система может оказаться уязвимой.

Сервис анализа защищенности приложений, предлагаемый «Лабораторией Касперского», позволяет выявить уязвимости в приложениях любого типа – от крупных облачных решений, ERP-систем, систем дистанционного банковского обслуживания и других бизнес-приложений до встроенных приложений и мобильных решений для различных платформ (iOS®, Android™ и др.).

Сочетание знаний, практического опыта и передовых международных методов позволяет нашим экспертам обнаруживать бреши в системе безопасности, которые делают вашу организацию уязвимой для следующих угроз:

- похищение конфиденциальных данных;
- получение несанкционированного доступа к системам и изменение данных;
- организация атак типа DoS (отказ в обслуживании);
- совершение мошеннических операций.

Наши рекомендации позволяют устранить обнаруженные уязвимости в приложениях и предотвратить подобные атаки.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

Сервис анализа защищенности приложений, предлагаемая «Лабораторией Касперского», помогает разработчикам и владельцам приложений:

- **избежать финансовых, операционных и репутационных потерь,** заблаговременно обнаруживая и устраняя уязвимости, посредством которых проводятся атаки на приложения;
- **сэкономить на устранении последствий,** обнаруживая уязвимости в приложениях на этапах разработки и тестирования, до внедрения системы в продуктивную среду, где исправление недостатков может быть связано с дополнительными расходами и необходимостью остановки бизнес-процессов;
- **организовать жизненный цикл безопасной разработки ПО** (S-SDLC), нацеленный на создание и сопровождение защищенных приложений;
- **выполнить требования государственных, отраслевых или внутренних корпоративных стандартов,** предусматривающих защиту приложений, например PCI DSS.

СОСТАВ РАБОТ И ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

В рамках сервиса могут оцениваться официальные веб-сайты и бизнес-приложения (стандартные или облачные), в том числе встроенные и мобильные приложения.

Состав сервиса подбирается индивидуально в соответствии с вашими потребностями и особенностями приложений. Он может включать:

- **анализ защищенности методом «черного ящика»**. Имитируются действия злоумышленника, действующего извне;
- **анализ защищенности «серого ящика»**. Имитируются действия внутренних пользователей с различным уровнем доступа;
- **анализ защищенности «белого ящика»**. Анализ с полным доступом к приложению, включая исходный код. Этот подход наиболее эффективен с точки зрения количества обнаруживаемых уязвимостей;

- **оценка эффективности системы превентивной защиты приложений (application firewall)**. Приложения проверяются в два этапа: с включенными и с выключенными механизмами защиты, чтобы эффективно выявить уязвимости и убедиться, что атаки выявляются и блокируются.

РЕЗУЛЬТАТЫ

Сервис анализа защищенности приложений, предлагаемый «Лабораторией Касперского», может обнаружить следующие уязвимости:

- недостатки аутентификации и авторизации, в том числе ошибки реализации двухфакторной аутентификации;
- инъекции кода (внедрение операторов SQL-инъекции, выполнение команд ОС и т. д.);
- уязвимости логики приложения, которые могут использоваться в мошеннических целях;
- уязвимости, приводящие к атакам на пользователей приложения (межсайтовое выполнение сценариев, подделка межсайтовых запросов и т. д.);
- использование слабых криптографических алгоритмов;
- уязвимости при обмене данными между клиентом и сервером;
- незащищенное хранение или передача данных, например отсутствие маскировки номеров PAN в платежных системах;
- ошибки конфигурации, в том числе делающие возможными атаки на сессии пользователей;
- раскрытие конфиденциальной информации;
- другие уязвимости в веб-приложениях, которые позволяют реализовать угрозы, перечисленные в классификации угроз WASC 2.0 и OWASP Top Ten.

Результаты работ представляются в виде итогового отчета с подробной технической информацией об обнаруженных уязвимостях и рекомендациями по их устранению, а также краткими выводами об уровне защищенности приложения. Кроме того, в случае необходимости могут быть подготовлены видеоматериалы и презентации для технических подразделений или руководства.

ПОДХОД «ЛАБОРАТОРИИ КАСПЕРСКОГО» К АНАЛИЗУ ЗАЩИЩЕННОСТИ ПРИЛОЖЕНИЙ

Анализ защищенности приложений проводится экспертами «Лаборатории Касперского» как с использованием автоматизированных средств, так и вручную. При этом предпринимаются все разумные меры предосторожности для сохранения конфиденциальности, целостности и доступности приложений.

«Лаборатория Касперского» строго следует международным стандартам и лучшим мировым практикам, среди которых:

- Web Application Security Consortium (WASC) Threat
- Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide

Специалисты, проводящие работы, – опытные профессионалы, обладающие обширными и актуальными практическими знаниями для различных платформ, языков программирования и методов атак. Они выступают на ведущих международных конференциях и известны своими исследованиями в области безопасности, в том числе обнаружением новых уязвимостей в крупнейших облачных сервисах и приложениях, включая Oracle, Google, Apple, Facebook, PayPal.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

В зависимости от метода анализа защищенности, особенностей тестируемой системы и требований клиента к условиям работы сервис анализа защищенности приложений может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно.

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для бизнеса:
www.kaspersky.ru/enterprise

+7 (495) 737-34-12
sales@kaspersky.com

KASPERSKY lab