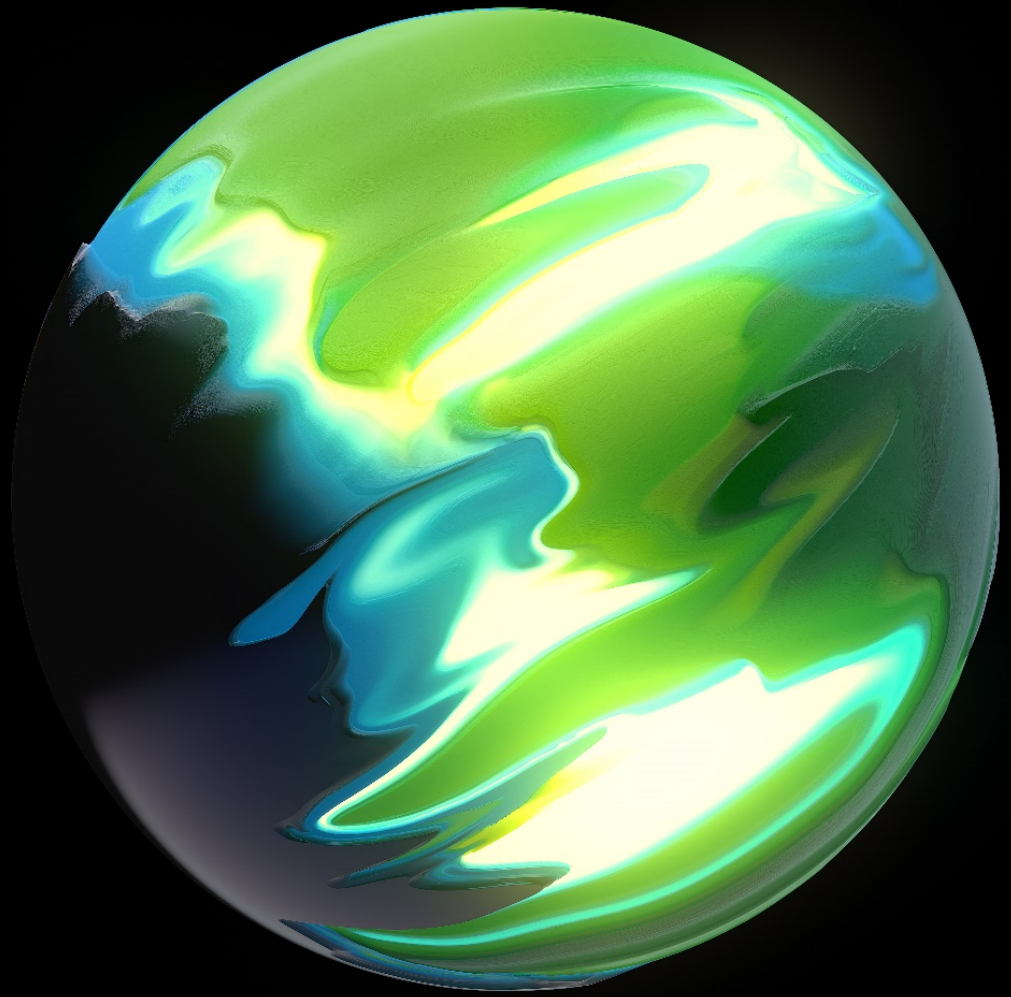
Deloitte.



Тестирование на проникновение в корпоративную сеть и оценка сопротивления целенаправленным атакам (Red Team)

Департамент управления рисками, 2021 год

MAKING AN IMPACT THAT MATTERS since 1845

Моделирование киберугроз

Экспоненциальный рост технологического оснащения и повсеместная компьютеризация привели к появлению новых типов риска, которые нельзя выявить при помощи традиционных способов тестирования защищенности. Каждый год растет число киберинцидентов, увеличиваются связанные с подобными атаками потери. Именно поэтому организациям необходимо демонстрировать готовность к реальным атакам, которые не ограничены рамками. Оценка защищенности информационных систем и веб-ресурсов, оценка осведомленности персонала в вопросах информационной безопасности и тестирование на возможность проникновения — это эффективные, но недостаточно гибкие инструменты, которые не охватывают поверхность реальной атаки полностью.

В соответствии с нашим подходом Red teaming включает:

- определение бизнес-целей исходя из негативного влияния потенциальных киберугроз;
- этапы пассивной и активной разведки;
- выявление наиболее релевантной «точки входа»;
- выявление наиболее эффективных и скрытых векторов развития атаки;
- подготовку программного обеспечения для обхода средств защиты;
- осуществление атаки, в том числе и «вглубь»;
- подготовку отчета.

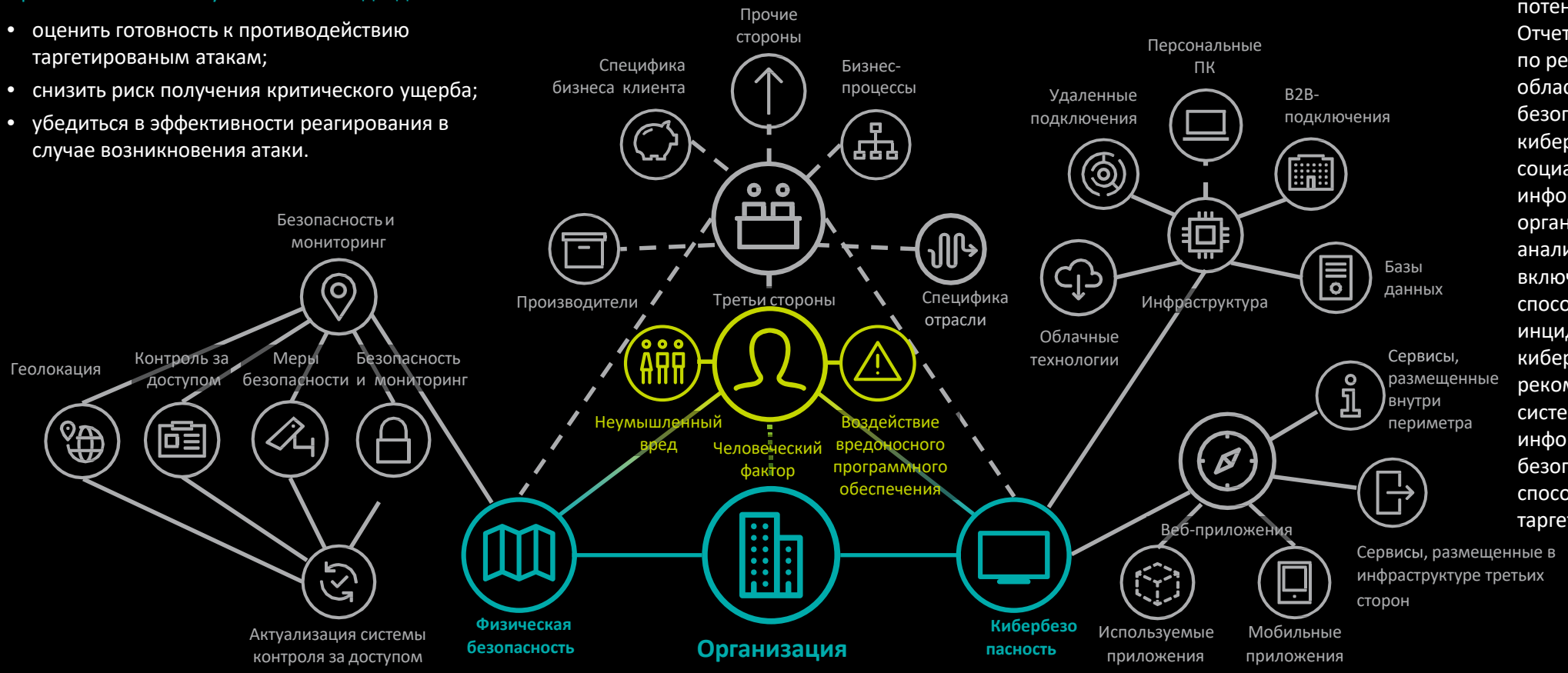
Red teaming — гибкое, целеориентированное и не ограниченное рамками тестирование, при котором не используются стандартные шаблоны и которое позволяет реализовать критичные векторы атак и тем самым оценить степень готовности к реагированию на инциденты. Данное тестирование предполагает попытку любым способом достичь целей, которые перед собой могут ставить злоумышленники: физический доступ, осуществление атак с применением социальной инженерии, скрытое тестирование на проникновение.

Поверхность атаки

Оценка возможностей по выявлению и реагированию — сложный и нестандартный процесс. Использование типовых приемов в ходе тестирования может значительно повлиять на результаты и уменьшить их достоверность. В ходе тестирования Red teaming мы не используем шаблоны, наша методология призвана объективно показать возможности организации по противостоянию сложным современным таргетированым атакам. Целью тестирования является не проверка всех возможных векторов, а определение критичных объектов воздействия, выявление максимально эффективных и скрытых векторов, проведение таргетированной контролируемой атаки с дальнейшим фиксированием и анализом результатов для последующего повышения общего уровня сопротивляемости угрозам.

Применение используемого нами подхода позволяет:

- оценить готовность к противодействию таргетированым атакам;
- снизить риск получения критического ущерба;
- убедиться в эффективности реагирования в случае возникновения атаки.

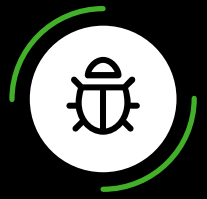


Многообразие субъектов, взаимодействующих с организацией, порождает большое количество связей, каждая из которых может нести в себе определенные угрозы, формируя потенциальные векторы атак. Отчет будет включать данные по результатам тестирования областей физической безопасности, кибербезопасности, а также социального фактора, информацию об актуальных для организации угрозах, аналитический раздел, включающий оценку рисков, способности к идентификации инцидентов и сопротивлению киберугрозам, а также перечень рекомендаций по укреплению системы информационной безопасности и улучшению способности противостоять таргетированым атакам.

Применяемые методы моделирования атак

Тестирование с учетом специфики организации представляет собой определение и реализацию векторов атак с учетом отраслевых особенностей деятельности, доступной в открытых источниках информации, касающейся наиболее критичных активов, бизнес-среды, ИТ- и физической инфраструктуры, а также общего уровня зрелости подразделения, отвечающего за кибербезопасность.

Наш подход предусматривает использование неразрушающих методов тестирования. В случае возникновения риска непрерывности деятельности мы проводим согласование планируемых шагов с ключевыми лицами, принимающими решения со стороны заказчика.



Эксплуатация известных уязвимостей
Пассивный и активный сбор информации, определение уязвимостей и их эксплуатация

Поиск необнаруженных уязвимостей и их эксплуатация
Тестирование путем подачи на вход некорректных параметров, поиск исходных кодов используемого программного обеспечения в свободном доступе, обратная разработка для поиска уязвимостей нулевого дня

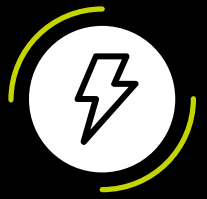
Получение доступа через вредоносное программное обеспечение
Определение диапазона IP- адресов организации, поиск вредоносной активности методами, лежащими в основе разведки на базе открытых источников, поиск операторов вредоносного программного обеспечения для приобретения доступа

Анализ электронных адресов и контактов
Выявление в открытых источниках корпоративных электронных адресов, телефонных номеров и персональных данных, которые могут быть использованы для осуществления атак

Осуществление инсайдерских атак
Выявление потенциальных инсайдеров на основе данных, доступных в открытых источниках, вхождение в контакт, формирование эффективного вектора и совершение атаки в соответствии с целями организации

Атаки с применением социальной инженерии
Активный и пассивный сбор информации, выявление наиболее эффективного вектора и осуществление атаки

Получение физического доступа
Тестирование контроля за доступом, мер обеспечения физической безопасности и систем мониторинга



Осуществление сетевых атак
Проведение атак типа «человек посередине» (атак, направленных на перехват данных), а также эксплуатация недостатков сетевой конфигурации

Осуществление атак с применением данных из открытых источников
Сбор данных из социальных сетей, анализ метаданных, поиск утечек и индексируемых критичных элементов для дальнейшего создания вектора и его реализации

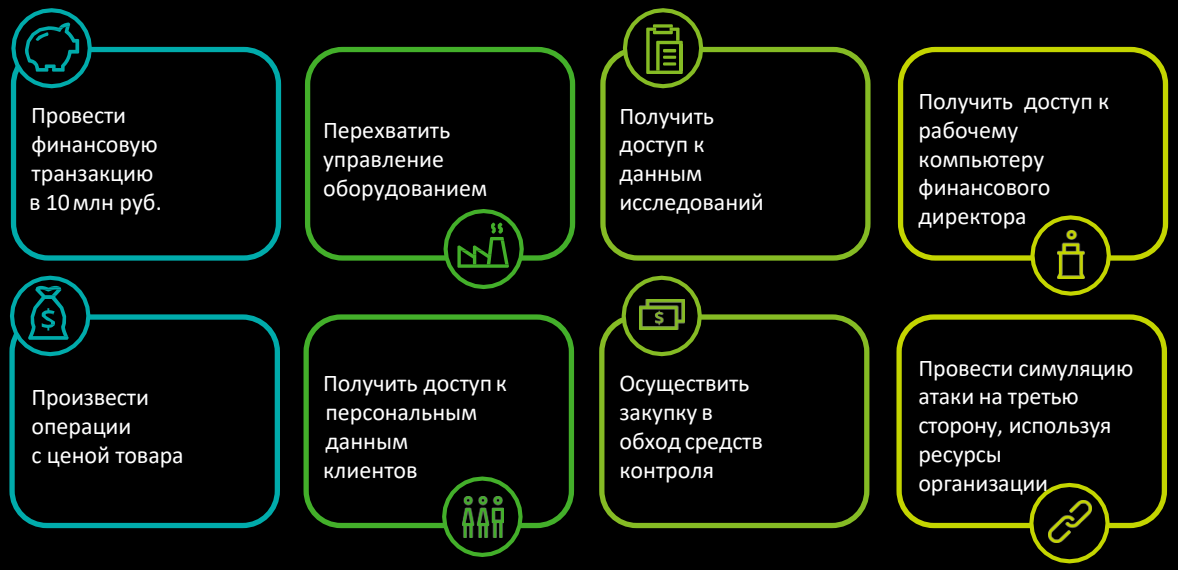
Совершение комбинированных атак
В ходе формирования перечня векторов мы комбинируем и корректируем применяемые методы для обеспечения соответствия целям организации

Реалистичный подход

Риски сложных атак не всегда можно выявить при помощи стандартных оценок защищенности. Контролируемые сценарии атак, покрывающие множество влияющих на безопасность аспектов, методологической основой которых являются общепринятые подходы, переориентированные на достижение конкретной цели, позволяют объективно оценивать эффективность работы команд защиты. В целях обеспечения максимальной реалистичности в выборе возможного вектора атаки и его реализации наши специалисты на регулярной основе анализируют цели, методы, способы и средства, используемые различными преступными группировками.

Кибербезопасность нельзя рассматривать отдельно от системы контрольных точек, включенных в бизнес-процессы для обеспечения надежности.
Необходимость построения многоуровневой системы защиты активов организации обусловлена негативным влиянием социального фактора. Наш подход позволяет объективно оценить надежность бизнес-среды, что дает возможность избежать возникновения инцидентов, спровоцированных социальным фактором, путем создания эффективной и отлаженной системы контрольных процедур на уровне бизнес-процессов.

Модель угроз



Ключевые принципы

Наши компетенции

Наша команда специалистов, участники которой в 2018 году заняли первое место на конкурсе этичных хакеров PHDays, а также в соревновании Cyberlympics в 2017, обладает богатым опытом проведения тестирований на проникновение, оценки соответствия конфигураций лучшей практике в сфере информационной безопасности и рекомендациям производителей, оценки защищенности и аудита информационной безопасности.

Квалификация наших специалистов подтверждается международными

сертификатами (CISSP, CISM, ISO27001, COBIT, ITIL, CDPP, CEH).

Компания Gartner признала «Делойт» лидером в категории Security Consulting шестой год подряд (источник: Gartner, Market Share Analysis: Security Consulting Services, Worldwide, 2017, Elizabeth Kim, 27 June 2018).

Как отмечают специалисты ALM Intelligence (исследовательская фирма, ранее известная как Kennedy), «Компания «Делойт» разрабатывает, тестирует и использует новые методологии, которые отражают глубокое понимание систем информационной безопасности клиентов и помогают компаниям создавать системы безопасности мирового уровня» (источник:

ALM Intelligence; Cybersecurity Consulting 2017; ALM Intelligence estimates © 2017 ALM Media Properties, LLC. Reproduced under license).

Контакты

Денис Липов

Партнер, Департамент управления рисками

dlipov@deloitte.ru

Тел.: +7 (495) 787 06 00, доб. 3071

Юлия Гончарова

Старший менеджер, Департамент управления рисками

ygoncharova@deloitte.ru

Тел.: +7 (495) 787 06 00, доб. 5086

Павел Черепанов

Старший консультант, Департамент управления рисками

pcherepanov@deloitte.ru

Тел.: +7 (383) 210 56 31, доб. 6239

Deloitte.