ХардкорIT

pt

DX

Программа трансформации ИТ для повышения киберустойчивости

!?

Как удлинить, усложнить и сделать заметнее продвижение хакера

Содержание

Каждую третью компанию можно взломать за 1 шаг

Недопустимое событие — событие, возникшее в результате кибератаки, которое делает невозможным достижение операционных и (или) стратегических целей организации или приводит к значительному нарушению ее основной деятельности.

Финансовый ущерб выше порогового значения — еще одно следствие реализации недопустимого события.

Чтобы оперативно оценить, сможет ли хакер причинить организации операционный, финансовый или репутационный ущерб, проводятся тесты на проникновение (пентесты) — моделирование реальных атак злоумышленников на инфраструктуру компании.

Такое тестирование позволяет выявить уязвимые места в элементах ИТ-инфраструктуры, практически продемонстрировать возможность использования уязвимостей и сформировать рекомендации по их устранению.

Но самое главное — пентест позволяет оценить возможность и скорость реализации недопустимого события в организации.

Сколько времени понадобится на взлом вашей компании?

5 дней

среднее время проникновения во внутреннюю сеть, а самая быстрая атака была проведена за 1 час

до 2 шагов

требуется для проникновения в локальную сеть в 57% организаций

≈10 дней

требуется для реализации недопустимого для бизнеса события

Данные основаны на результатах 53 проектов по тестированию на проникновение, проведенных в 30 российских организациях. Более половины (57%) исследованных предприятий входят в рейтинг крупнейших компаний России по объему реализации продукции RAEX-600.

ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/

Уязвимая конфигурация ИТ-инфраструктуры

Основная причина проблем

Эксперты Positive Technologies выявили ключевые недостатки конфигурации ИТ-инфраструктуры, приводящие к успешным кибератакам:

- ☐ слабая парольная политика
- ☐ недостатки конфигураций веб-приложений
- ☐ уязвимости в коде приложений
- ☐ недостатки конфигураций почтовых систем
- ☐ отсутствие актуальных обновлений
- ☐ избыточные права доступа
- ☐ отсутствие двухфакторной аутентификации для доступа к критически важным ресурсам
- ☐ хранение аутентификационной информации в открытом виде
- ☐ использование устаревших протоколов доступа
- ☐ недостатки сетевой безопасности
- ☐ недостатки конфигураций средств аутентификации
- ☐ возможность обхода средств защиты

Большинство проблем из этого списка может быть устранено при помощи настройки ИТ-инфраструктуры в компании

Харденинг — защита инфраструктуры путем снижения рисков от возможных киберугроз за счет реконфигурации сетевой инфраструктуры и приложений.

Вот почему мы разработали методологию, которая рассматривает задачи обеспечения киберустойчивости как часть задач ИТ и позволяет компаниям защититься от недопустимых событий.

Усложнить путь хакера —

Первый шаг к результативной кибербезопасности

Любая кибератака заключается в последовательном продвижении атакующего к целевой системе, где выполняется запланированное пагубное действие.

Такое продвижение состоит в последовательности шагов: от узла к узлу, от системы к системе, от периметра к ядру сети. Как и в реальном мире, каждый шаг требует от атакующего усилий и оставляет следы. Задача защитника — сделать это движение более трудным, долгим, затратным, а также более «шумным», чтобы атакующего можно было заметить как можно раньше.

Результативная кибербезопасность — состояние защищенности организации, которое обеспечивает ее устойчивость к кибератакам и позволяет в любой момент на практике подтвердить, что злоумышленник не сможет реализовать недопустимые для этой организации события.

Поэтому наша задача — удлинить цепочку шагов и действий атакующего, заставить его использовать наиболее сложные техники, оставляющие много признаков компрометации и затратные по времени. Это позволяет сильно увеличить время совершения кибератаки и ускорить реагирование так, чтобы атакующий был обнаружен и заблокирован в ИТ-инфраструктуре до реализации недопустимого события. Такие действия — первый шаг к результативной кибербезопасности.

Первая методология повышения киберустойчивости средствами ИТ

Киберустойчивость — способность информационной системы организации, отрасли или государства непрерывно функционировать в условиях кибератак.

«ХардкорИТ» — это методология определения времени и путей атаки хакера методом анализа ИТ-инфраструктуры.

Она подразумевает под собой эффективную и быструю оценку защищенности конкретных ИТ-систем, критически важных для бизнеса, а также повышение киберустойчивости компании за счет:

- **максимального использования встроенных механизмов защиты ИС**
- **повышения кибергигиены (патч-менеджмента, парольных политик и т.д.)**

«ХардкорИТ» реализуется через выполнение шагов

1. Формулирование недопустимых для бизнеса компании событий.
2. Декомпозиция недопустимого события на сценарии его реализации.
3. Определение ключевых (доступ к которым упрощает хакеру продвижение к цели) и целевых систем (конечной цели хакера).
4. Анализ текущей ИТ-инфраструктуры с точки зрения задач кибербезопасности.
5. Моделирование атак и расчет ключевых метрик киберустойчивости.
6. Формирование и реализация программы внедрения контролей безопасности.
7. Сравнительный анализ основных метрик киберустойчивости для текущего и целевого состояний ИТ-инфраструктуры.
8. Проведение кибериспытаний для оценки достигнутого результата.

*Эти шаги — часть методики результативной кибербезопасности, но они необходимы на пути на трансформации ИТ.

ХардкорИТ

Особенности методологии

Вовлечение ИТ-подразделений в повышение киберустойчивости компании.

Объединение экспертизы Positive Technologies и лучших мировых практик.

Наличие видимых и измеримых улучшений («быстрых побед») для достижения киберустойчивости компании.

Максимальное использование встроенных механизмов защиты в ОС, СУБД и приложениях.

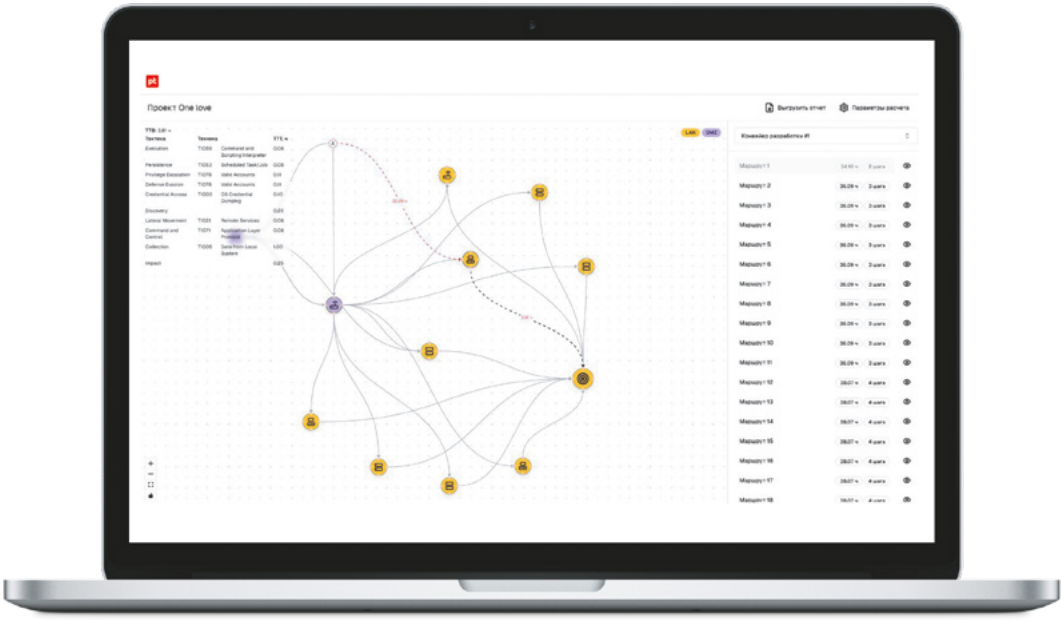
Моделирование действий хакера на основе гранулярной информации об использовании конкретных механизмов защиты.

Выявление систем, которые представляют наибольший интерес для атакующего, на основе анализа сценариев недопустимых событий.

Расчет времени прохождения атаки на основании экспертизы Positive Technologies.

Оценка достаточности примененных контролей безопасности и расчет количественных показателей (метрик) киберустойчивости.

На последнем этапе — формирование стратегии трансформации ИТ-инфраструктуры с учетом полученных данных и с целью предотвращения недопустимых событий.



Граф достижимости: цифровая модель помогает рассчитать время самой быстрой реализации атаки, обозначить техники MITRE ATT&CK, найти недостатки конфигурации ИТ-инфраструктуры, отобразить точки, в которых злоумышленник может быть остановлен, и ИТ-активы, через которые может проходить наибольшее количество атак.

Результаты

1

Сформирована программа трансформации ИТ для построения результативной кибербезопасности.

2

По итогам реализации программы трансформации ИТ количество доступных атакующему путей уменьшено, ведущие к целевым системам пути удлинены, а следование по ним стало более сложным для любого атакующего.

Рост затрат времени и усилий на достижение целей атакующего *(TTA – время на атаку)* будут приводить к отказу от продолжения атаки и росту наших возможностей для ее обнаружения и прекращения до нанесения неприемлемого ущерба.

3

Компания также получает рекомендации по снижению времени обнаружения и реагирования на действия атакующего *(TTC – время локализации угрозы)*, что в комплексе с высоким TTA приведет к практической невозможности реализации недопустимых событий.

Почему Positive Technologies

Опыт

Эксперты компании провели более 500 оценок защищенности и расследований инцидентов ИБ, проанализировали тактики злоумышленников, векторы проникновения, векторы развития и техники закрепления в ИТ-инфраструктуре. Весь этот опыт лежит в основе предлагаемой методологии.

База знаний

Собранная нами база знаний «ХардкорИТ» основана на глубокой экспертизе компании в пентестах, расследовании инцидентов и их аналитики и помогает создавать продукты для кибербезопасности, отвечающие потребностям компаний в современном ландшафте угроз.

Команда

Эксперты «ХардкорИТ» создают программы трансформации и проводят авторский надзор за реализацией проектов партнерами. Опыт в создании разных критических ИТ-инфраструктур позволяет нам разрабатывать оптимальные схемы харденинга для каждого клиента и проекта, а накопленный в этих проектах опыт используется в метапродуктах PT.

pt@ptsecurity.com

Свяжитесь с менеджером Positive Technologies, чтобы получить персональную консультацию.

Хотите познакомиться с практическим применением методологии?

«Руководство по защите MS Exchange 2019»

ptsecurity.com

Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.

Наши технологии используют более 4000 организаций по всему миру.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.