Оглавление

Введение

Повышение осведомлённости сотрудников информационной безопасности - обязательное условие для обеспечения и поддержания кибербезопасности предприятия на высоком уровне, ведь обучение - это не только документальное подтверждение наличия знаний, но и возможность узнать о новых киберугрозах и способах борьбы с ними.

Способы повышения осведомлённости прошли эволюцию от лекций и лабораторных работ в учебных центрах до соревнований между «Защищающей» и «Атакующей» командами. Очередной этап этой эволюции — специализированные киберполигоны, где можно не только провести анализ защищённости путём сканирования ИТ-активов на возможные уязвимости, но и довести атаку до логического окончания и, например, остановить реактор атомной станции.

Киберполигоны — платформы для профессиональных технических киберучений, где можно обучать сотрудников, входящих в “Защитную” или “Атакующую” команду. Киберполигоны позволяют смоделировать реальную ИТ-инфраструктуру предприятия и оценить возможность её взлома, а также готовность к защите от кибератак.

Комплексы для обучения противодействию кибератакам

Сильная сторона использования симуляции атак на ИТ-инфраструктуру компании более чем очевидна. Маловероятно, что руководство компании для проверки готовности подразделений ИБ согласиться попасть под атаку “этичных” хакеров. Если что-то во время учений пойдёт не так, то это будет чревато потенциальными проблемами при восстановлении инфраструктуры, возможным простоем бизнес-процессов. В то же время на специализированном полигоне всё это можно проделать без ущерба для бизнеса, смоделировав необходимую инфраструктуру.

Во время работы на полигоне ответственные за обеспечение кибербезопасности и работоспособность ИТ подразделения на практике проверяют, могут ли они заблаговременно обнаружить индикаторы нанесение вреда инфраструктуре либо развивающуюся атаку до того, как она дойдёт до финальной стадии, жизнеспособны ли разработанные на этот случай регламенты, налажено ли взаимодействие, понимает ли ИТ проблемы ИБ и наоборот.

Итогом проводимых киберучений может быть проверка не только того, как ИТ и ИБ реагируют на атаки злоумышленников, но и того, как действуют другие подразделения атакуемой компании: например, за какое время пресс-служба сможет выпустить релиз об инциденте для минимизации

репутационных потерь, а юридический департамент — собрать необходимые данные для подачи заявления в правоохранительные органы или страховую компанию.

Тренинги на киберполигонах подходят не только большим компаниям с развитой инфраструктурой, но и малым предприятиям. Главные условия — это уровень зрелости соответствующих процессов, понимание того, для чего нужен подобный тренинг, и системный подход при подведении итогов. Это позволит сформировать план мероприятий для повышения уровня защищённости компании.

Несмотря на незначительное время популярности направления, уже есть разделение платформ в зависимости от поколений: традиционные киберполигоны и киберполигоны следующего поколения. Главное отличие состоит в возможностях, предоставляемых этими платформами. Традиционные киберполигоны представляют собой набор смоделированных систем, на которые производится атака, в то время как киберполигоны нового поколения включают в себя множество дополнительных сервисов и возможностей: симуляция действий обычных пользователей, различные инструменты для преподавателя, сбор и анализ данных.

В связи с нарастающей популярностью направления, создаются фестивали, конкурсы и шоу по киберполигонам. На данный момент были проведены такие мероприятия как: Интеллектуальное онлайн-шоу о кибербезопасности и IT “КиберАрена”, киберквест на киберполигоне Ampire, Cyber Polygon 2021, ”Киберполигон”.

Российский рынок комплексов для обучения противодействию кибератакам

Российский рынок киберполигонов менее насыщен, чем зарубежный, но имеет тенденцию к росту. Совсем недавно, власти РФ потратили 1,9 млрд руб. на создание и развитие в России «Национального киберполигона» для тренировок и обучения специалистов в области информационной безопасности. Проект реализуется компанией «Ростелеком-Solar». В рамках киберполигона отрабатываются сценарии для банковской, нефтяной, энергетической отраслях, в планах расширение полигона на нефтепереработку и магистральные сети связи.

Киберполигон состоит из пяти крупных блоков: платформа для киберучений «Кибермир», подсистема автоматизированного проведения кибератак, подсистема автоматической оценки действий участников, эмуляция технологических и бизнес-процессов и подсистема инфраструктуры. Сама инфраструктура, в свою очередь, включает виртуальные образы, реальное физическое оборудование и полунатурное моделирование. В

совокупности все эти элементы позволяют погружать участников в интерактивную среду с актуальными именно для их специализации и отрасли атаками.

Помимо “Национального киберполигона”, также в России присутствуют такие платформы для проведения киберучений как:

- Ampire (Компания “Перспективный мониторинг”)
- BI.ZONE (Компания “Сбербанк”)
- Jet CyberCamp.
- The Standoff (Компания “Positive Technologies”)
- “Киберполигон” (ООО “Киберполигон”)

Зарубежный рынок комплексов для обучения противодействию кибератакам

Зарубежный рынок киберполигонов не стоит на месте. Существует множество продвинутых иностраных комплексов по обучению противодействию кибератакам с разными подходами. Например, киберполигон Check Point Cyber Range компании Check Point построен по принципу игры, позволяющее сделать обучение интересным. Киберполигон предназначен для обеих сторон противостояния – как атакующих, так и защитников.

Процесс обучения затрагивает уязвимости разных уровней: операционной системы, приложений и веб-приложений. Также он охватывает работу с решениями Check Point для защиты сети предприятия от кибератак.

Также нельзя не упомянуть следующие зарубежные платформы для проведения киберучений:

- Cisco Cyber Range, демонстрирующий более 100 реальных атак на предприятие.
- Cyber Ranges, официальной платформы международного союза электросвязи
- Project Ares, геймифицированный курс прохождения обучения

Заключение

Востребованность киберучений по противодействию кибератакам на данный момент возрастает и будет постоянной. Компании хотят защитить свою ИТ-инфраструктуру от атак, так как незаблаговременное обнаружение и защита чревато простоями бизнес-процессов, кражей важных данных,

потенциальными проблемами при восстановлении инфраструктуры, репутационными последствиями.

Список литературы

[1] Обзор рынка киберполигонов. https://www.anti-malware.ru/analytics/Market_Analysis/Cyber-Polygons#part1. 19.10.2022

[2] cnews.ru. https://safe.cnews.ru/news/top/2022-09-06_vlasti_potratyat_19_milliarda. 19.10.2022.