СОЗДАНИЕ СТРАТЕГИИ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Любчик Д.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пулко Т.А. – канд. тех. наук, доцент

Каждый день в информационных системах обнаруживается множество новых уязвимостей, причем обнаруживаются они как с целью их исправления, так и для их эксплуатации. Исправляются уязвимости часто после обнаружения факта их использования. К моменту исправления, общий ущерб от эксплуатации уязвимости является значительным. Это обязывает к созданию процесса управления уязвимостями, который можно использовать для их выявления и нейтрализации.

Оптимальный подход к созданию эффективной стратегии управления уязвимостями - сделать ее жизненным циклом управления уязвимостями. Как и жизненный цикл атаки, жизненный цикл управления уязвимостями упорядочено планирует все процессы по их нейтрализации. Это позволяет целям и жертвам инцидентов, связанных с кибербезопасностью, нейтрализовать ущерб, который они понесли [1].

Стратегия управления уязвимостями состоит из шести отдельных этапов. Первым этапом в стратегии управления уязвимостями должно быть проведение инвентаризации активов. Но во многих организациях отсутствует либо содержится не полный реестр активов, поэтому они испытывают трудности при защите своих устройств. При создании стратегии управления уязвимостями, организация должна начать с того, чтобы сделать одного из сотрудников ответственным за инвентаризацию активов с целью гарантировать, что все устройства зарегистрированы и что результат инвентаризации всегда актуален [2]. Без этого о некоторых устройствах можно забыть при исправлении или установке нового программного оборудования, используемого для обеспечения безопасности. Это устройства и системы, на которые будут нацелены злоумышленники. Организациям также не хватает эффективных инструментов, чтобы поддерживать инвентаризацию в согласованном порядке. Обновленный реестр активов пригодится, когда организации придется реагировать на уязвимости, исправляя все свои ресурсы.

Вторым этапом стратегии управления уязвимостями является управление информацией, т.е. контроль того, как информация поступает в организацию. Наиболее важной информацией является интернет-трафик, поступающий из сети организации. Кроме того, организации хранят различные типы данных, и некоторые их них ни в коем случае не должны попасть в руки злоумышленников. Если к коммерческой тайне и личной информации клиентов получат доступ хакеры. это может нанести непоправимый ущерб. Организация может лишиться своей репутации и потерять клиентов. Следовательно, управление информацией имеет жизненно важное значение в стратегии управления уязвимостями. На данном этапе также должно стать создание эффективного способа передачи информации об уязвимостях и инцидентах в области кибербезопасности соответствующим лицам в кротчайшие сроки. На этом этапе существует несколько проблем. Одна из проблем в том, что с годами объемы информации в организации постоянно увеличивается, что усложняет работу с ней, а также контроль над доступом к ней. Ценная информация, касающаяся взломов, такая как оповещения, также может превышать возможности обработки большинства IT-отделов. Релевантные оповещения об атаках могут отбрасываться как ложные срабатывания из-за количества аналогичных оповещение, которые возникают ежедневно. Также возникает проблема, когда речь идет о передаче информации о новых уязвимостях обычным пользователям, которые не разбираются в технических особенностях. Все это влияет на время отклика и действия, которые организация может предпринять в случае потенциальных или проверенных попытках взлома.

Оценка рисков является третьим этапом в стратегии управления уязвимостями. Прежде чем риски могут быть уменьшены, требуется проведение углубленного анализа уязвимостей. В идеальных условиях сотрудники по обеспечению безопасности в организации могут реагировать на все уязвимости, поскольку у нее достаточно ресурсов и времени. Однако в действительности существует очень много ограничивающих факторов. Вот почему оценка рисков имеет решающее значение. Оценка рисков должна сопровождаться оценкой уязвимостей. На этом этапе организация должна растравить приоритеты одних уязвимостей над другими и выделить ресурсы для их устранения. Оценка рисков также должна состоять из шести этапов:

- область действия;
- сбор данных;
- анализ политик и процедур;
- анализ уязвимостей;

- анализ угроз;
- анализ приемлемых угроз.

Четвертым этапом является оценка уязвимостей. Она тесно связана с оценкой риска на предыдущем этапе. Оценка уязвимостей включает в себя выявление уязвимых ресурсов. Эта фаза проводится с помощью ряда согласованных попыток взлома и тестов на проникновение. Цель состоит в том, чтобы смоделировать реальный сценарий взлома с использованием тех же инструментов и методов, которые может использовать потенциальный злоумышленник. Требуется получить исчерпывающий отчет обо всех уязвимостях, которые есть. На на данном этапе существует несколько проблем. Без соответствующей инвентаризации активов нельзя будет определить, на каких устройствах следует сосредоточиться. Также можно забыть оценить защищенность отдельных хостов, а они тем не менее могут оказаться ключевыми целями для потенциальной атаки. Другая проблема связана с используемыми сканерами уязвимостей. Некоторые сканеры могут предоставлять неверные отчеты об оценке уязвимостей. Но ложные срабатывая в сканерах будут всегда. Важно чательно анализировать отчет, иначе это может привести к растрате ресурсов в организации, когда дело доходит до мер по исправлению уязвимостей.

После оценки уязвимостей следующим этапом является стадия отчетов и исправлений. Этот этап имеет две одинаково важные задачи: отчеты и исправление ошибок. Отчеты помогают системным администраторам понять текущее состояние безопасности в организации и области, где она все еще уязвима. Отчеты обычно создается до момента исправления уязвимостей, чтобы вся информация, собранная на этапе управления уязвимостями, могла беспрепятственно перетекать в этот этап. Исправление запускает реальный процесс завершения цикла управления уязвимостями. Этап управления уязвимостями преждевременно заканчивается после анализа угроз и уязвимостей, а также определения приемлемых рисков. Исправление дополняет это, предлагая решения для противодействия выявленным угрозам и уязвимостям. Все уязвимые ресурсы отслеживаются, после чего принимаются необходимые меры для устранения уязвимостей, а также защиты от последующих эксплойтов. Это самая важная задача в стратегии управления уязвимостями, и если она выполнена надлежащим образом, управление уязвимостями считается успешным. Но на данном этапе также встречается множество проблем, поскольку именно здесь определяются решения для всех уязвимостей. Первая проблема возникает, когда отчеты не покрывают все необходимые сферы и не содержат нужной информации о рисках, с которыми сталкивается организация. Плохо написанный отчет может привести к слабым мерам по исправлению и оставить организацию по прежнему уязвимой к угрозам. Также, процесс исправления может быть поставлен под угрозу из-за отсутствия сотрудничества конечных пользователей. Исправление может привести к простоям, а это то, что пользователям абсолютно не нужно.

Планирование реагирования можно рассматривать как самый простой, но тем не менее очень важный этап в стратегии управления уязвимостями. Он не предоставляет проблем, потому что вся важная работа была проделана на предыдущих этапах. Это важно потому что без него организация по прежнему будет подвержена угрозам. На этом этапе важна только скорость исполнения. Крупные организации сталкиваются с серьезными препятствиями при выполнении из-за большого количества устройств, которые требуют исправлений и обновлений. После выпуска исправлений хакеры быстро пытаются найти способы скомпрометировать организации, в которых их не устанавливали. Это показывает, насколько важна скорость, когда речь идет о планировании реагирования. Исправления должны устанавливаться в тот момент, когда они станут доступны [1]. При планировании реагирования организация должна предложить средства исправления или обновления систем, которые были определены как имеющие определенные риски или уязвимости. Следует придерживаться иерархии серьезности угроз, определенной на этапах оценки риска и уязвимостей. Этот шаг должен быть реализован с помощью инвентаризации активов, чтобы организация могла подтвердить, что были задействованы все ее ресурсы, как аппаратные, так и программные. Этап планирования реагирования должен быть завершен с учетом того, когда системы мониторинга отправляют оповещения тем, кто реагирует на инциденты.

Таким образом, организации оказываются под давлением необходимости быстро реагировать на динамично растущее число угроз в области кибербезопасности. Поскольку злоумышленники использовали жизненный цикл атаки, организации также были вынуждены разработать жизненный цикл управления уязвимостями. Он предназначен для противодействия усилиям злоумышленников самым быстрым и эффективным методом.

Список использованных источников:

1. Диогенес Ю, Озкайя Э. Кибербезопасность: стратегии атак и обороны. – М. : Изд-во ДМК, 2020 . – 323 с.

2. Rawan K.. Today’s Inventory Management Systems: A Tool in Achieving Best Practices in INdian Business // Anusandhanika, 2015. №7 – P. 128-135.