НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Йомудова Джахан

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Гылычдурдыева Чынар

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Репова Аннагозел

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Илясов Аннамерет

Студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Для анализа проблем кибербезопасности, с которыми сталкиваются компании в настоящее время, необходимо получить реальные данные и доказательства того, что в настоящее время происходит на рынке. Не во всех отраслях будут одинаковые проблемы в области кибербезопасности. По этой причине мы перечислим угрозы, которые по-прежнему наиболее распространены в различных отраслях. Это кажется самым подходящим подходом для аналитиков кибербезопасности, не специализирующихся на определенных отраслях, но в какой-то момент своей карьеры им, возможно, придется иметь дело с определенной отраслью, с которой они не очень знакомы.

Старые методы и более широкие результаты

Согласно отчету о глобальных рисках в сфере IT от лаборатории Касперского за 2016 г, основные причины наиболее дорогостоящих утечек данных связаны со старыми атаками, которые развиваются с течением времени в следующем порядке:

-вирусы, вредоносные программы и трояны;

-недостаток усердия и неподготовленность сотрудников;

-фишинг и социальная инженерия;

-целевая атака;

-программы-вымогатели.

Хотя первые три в этом списке – старые знакомые и хорошо известны в сообществе кибербезопасности, они все еще преуспевают и по этой причине являются частью текущих проблем. Настоящая проблема состоит в том, что обычно они связаны с человеческими ошибками. Как объяснялось ранее, все может начинаться с фишингового сообщения по электронной почте, использующего социальную инженерию, чтобы заставить сотрудника щелкнуть ссылку, которая может загрузить вирус, вредоносное ПО или троян. В последнем предложении мы рассмотрели всех троих в одном сценарии.

Термин целевая атака (или продвинутая постоянная угроза) иногда не слишком понятен отдельным лицам, но есть некоторые ключевые атрибуты, которые могут помочь вам определить этот тип атаки. Первый и самый важный атрибут заключается в том, что у злоумышленника есть конкретная цель, когда он или она начинает составлять план атаки.

Во время этой начальной фазы злоумышленник потратит много времени и ресурсов на проведение публичной разведки для получения информации, необходимой для осуществления атаки. Мотивом для этой атаки обычно является эксфильтрация данных, другими словами, их кража. Еще один атрибут этого типа атаки – срок службы или период времени, в течение которого они поддерживают постоянный доступ к сети цели.

Намерение злоумышленника состоит в том, чтобы продолжать дальнейшее распространение по сети, взламывая различные системы, пока цель не будет достигнута.

Одна из самых больших проблем в этой области – идентификация злоумышленника, когда он уже находится в сети. Традиционных систем обнаружения, таких как системы обнаружения вторжений (IDS), может быть недостаточно для оповещения о подозрительных действиях, особенно при шифровании трафика. Многие специалисты уже отмечали, что между проникновением и обнаружением может пройти до 229 дней. Сокращение этого разрыва, безусловно, является одной из важнейших задач для специалистов в области кибербезопасности.

Программы-вымогатели – это новые и растущие угрозы, которые создают совершенно новый уровень проблем для организаций и специалистов по кибербезопасности. В мае 2017 г. мир был потрясен крупнейшей в истории атакой с использованием программы-вымогателя под названием Wannacry. Вирус эксплуатировал известную уязвимость в Windows, SMBv1, исправление для которой было выпущено в марте 2017 г. (за 59 дней до атаки) в бюллетене MS17-010 (16). Злоумышленники использовали эксплойт EternalBlue, выпущенный в апреле 2017 г. хакерской группой Shadow Brokers. Согласно MalwareTech (18), этот вымогатель заразил свыше 400 000 компьютеров по всему миру. Это гигантская цифра, которой никогда не наблюдалось в подобных атаках. Один из уроков, извлеченных в ходе этой атаки, заключался в том, что компаниям по всему миру по-прежнему не удается внедрить эффективную программу управления уязвимостями, о чем мы более подробно расскажем в главе 15 «Управление уязвимостями».

Очень важно отметить, что фишинговые письма по-прежнему являются средством доставки номер один для программ-вымогателей, а это означает, что мы снова возвращаемся к тому же циклу обучения пользователя, чтобы снизить вероятность успешной эксплуатации человеческого фактора с помощью социальной инженерии и иметь жесткие технические средства контроля безопасности для защиты от угроз и их обнаружения.

Улучшение стратегии безопасности

Если вы внимательно прочитаете всю эту главу, то совершенно четко поймете, что нельзя использовать старый подход к безопасности в противостоянии сегодняшним вызовам и угрозам. По этой причине важно убедиться, что ваша система безопасности готова справиться с этими проблемами. Для этого вы должны укрепить текущую систему защиты на разных устройствах независимо от форм-фактора.

Также важно, чтобы IT-отделы и службы безопасности могли быстро идентифицировать атаку, улучшив систему обнаружения. И последнее, но не менее важное: необходимо сократить время между заражением и сдерживанием, быстро реагируя на атаку путем повышения эффективности процесса реагирования.

Исходя из этого, можно с уверенностью сказать, что стратегия безопасности состоит из трех основных столпов, как показано на рис. 1

Эти столпы нужно укреплять, и если в прошлом большая часть бюджета направлялась на защиту, то теперь существует еще большая необходимость распределять эти инвестиции и объем работ по другим областям. Эти инвестиции не относятся исключительно к техническому контролю безопасности, они также должны осуществляться в других сферах бизнеса, включая административный контроль.

Рекомендуется выполнить самопроверку, чтобы определить пробелы в каждом столпе с инструментальной точки зрения. Многие компании развивались с течением времени и никогда не обновляли свои средства безопасности, чтобы приспособиться к новой среде угроз и тому, как злоумышленники эксплуатируют уязвимости.

Компания, где большое внимание уделяется вопросам безопасности, не должна быть частью ранее упомянутой статистики (229 дней между проникновением и обнаружением). Этот разрыв должен быть резко сокращен, а ответ должен быть немедленным.

Чтобы достичь этого, нужно разработать процесс реагирования на инциденты с использованием передовых и современных инструментальных средств, которые могут помочь инженерам по безопасности исследовать связанные с безопасностью проблемы.

В связи с возникающими угрозами и проблемами в области кибербезопасности необходимо было изменить методологию, перейдя с модели «предотвратить взлом» (prevent breach) на модель «подразумевать взлом» (assume breach). Традиционный подход «предотвратить взлом» сам по себе не способствует непрерывному тестированию, и для борьбы с современными угрозами всегда нужно совершенствовать свою защиту. По этой причине принятие данной модели в области кибербезопасности было естественным шагом.