НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

ЛАНДШАФТ КИБЕРУГРОЗ

Сопыева Огулбайрам

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

Бабаджанов Мердан

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

С преобладанием постоянных подключений и достижений в технологиях, которые доступны на сегодняшний день, киберугрозы быстро развиваются, чтобы эксплуатировать различные аспекты этих технологий. Любое устройство уязвимо для атаки, а с появлением концепции «интернета вещей» (IoT) это стало реальностью. В октябре 2016 г. на DNS-серверы была проведена серия DDos-атак, в результате чего перестали работать некоторые основные веб-сервисы, такие как GitHub, Paypal, Spotify, Twitter и др.

Это стало возможным из-за большого количества небезопасных IoT-устройств по всему миру. В то время как использование IoT для запуска масштабной кибератаки является чем-то новым, наличие уязвимости в этих устройствах таковым не является. На самом деле они были там довольно давно. В 2014 г. компания «ESET» сообщила о 73 000 незащищенных камерах безопасности с паролями по умолчанию. В апреле 2017 г. компания «IOActive» обнаружила 7000 уязвимых маршрутизаторов Linksys, хотя, по ее словам, число дополнительных маршрутизаторов могло доходить до 100 000.

Главный исполнительный директор (CEO) может даже спросить: какое отношение уязвимости в домашнем устройстве имеют к нашей компании? Именно в этот момент главный специалист по информационной безопасности (CISO) должен быть готов дать ответ. Ведь у него должно быть лучшее понимание ландшафта киберугроз и того, как домашние устройства пользователей могут влиять на общую безопасность. Ответ приходит в виде двух простых сценариев, таких как удаленный доступ и Bring your Own Device (BYOD).

Хотя удаленный доступ не является чем-то новым, число удаленных работников растет в геометрической прогрессии. По данным Gallup (4), 43 % занятых американцев уже работают удаленно, а это означает, что они используют свою собственную инфраструктуру для доступа к ресурсам компаний. Усугубляет эту проблему рост числа компаний, разрешающих концепцию BYOD на рабочем месте. Имейте в виду, что существуют способы безопасного внедрения BYOD, но большинство сбоев в сценарии BYOD обычно происходит из-за плохого планирования и сетевой архитектуры, которые приводят к небезопасной реализации.

Что общего между всеми вышеупомянутыми технологиями? Чтобы управлять ими, нужен пользователь, и он по-прежнему является главной целью для атаки. Люди – самое слабое звено в цепи безопасности.

По этой причине старые угрозы, такие как фишинговые электронные письма, продолжают расти в объеме, поскольку они затрагивают психологические аспекты пользователя, побуждая его кликнуть что-либо, например вложение файла или вредоносную ссылку. Обычно, когда пользователь выполняет одно из этих действий, его устройство заражается вредоносным ПО или к нему удаленно получает доступ хакер.

Таргетированная фишинговая кампания (spear phish) может начаться с электронного письма, которое, по сути, станет отправной точкой для злоумышленника, после чего будут использованы другие угрозы для эксплуатации уязвимостей в системе.

Одними из примеров растущей угрозы, которая использует фишинговые письма в качестве отправной точки для атаки, являются программы-вымогатели (ransomware). По сообщениям ФБР, только в течение первых трех месяцев 2016 г. вымогателям было выплачено 209 млн долларов. По данным компании «Trend Micro», рост числа атак с использованием программ-вымогателей стабилизировался в 2017 г. Тем не менее методы атаки и цели варьируются.

На рис. 1.1 показана взаимосвязь между этими атаками и конечным пользователем.

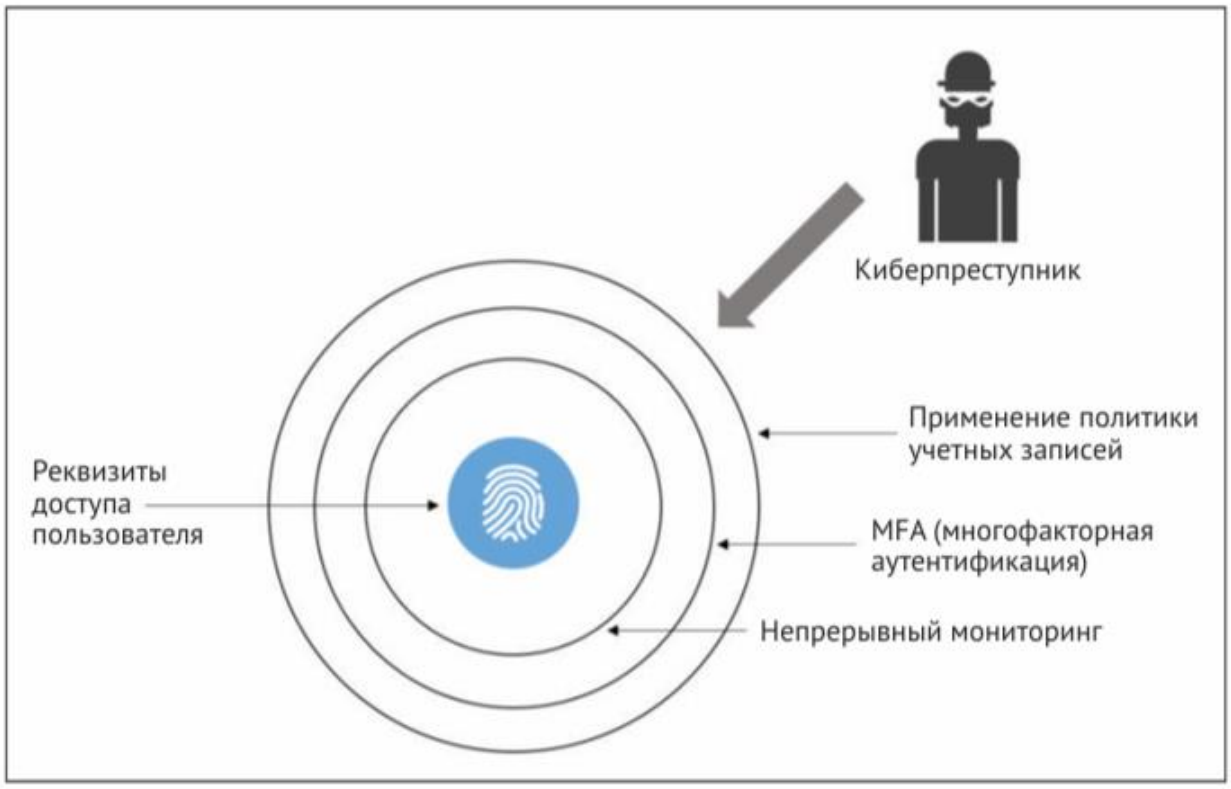
Эта диаграмма показывает четыре точки входа для конечного пользователя. Все они должны иметь свои риски, идентифицированные и обработанные с надлежащим контролем. Сценарии перечислены следующим образом:

-связь между локальными и облачными ресурсами (1);

-связь между BYOD-устройствами и облачными ресурсами (2);

-связь между корпоративными устройствами и локальными ресурсами (3);

-связь между персональными устройствами и облачными (4).



Еще одной растущей тенденцией для защиты личных данных пользователей является применение многофакторной аутентификации. Один из методов, который получил более широкое распространение, – это функция обратного вызова, когда пользователь первоначально аутентифицируется, используя свои учетные данные (имя пользователя и пароль), и получает вызов для ввода своего пин-кода. Если оба фактора аутентификации успешны, им разрешен доступ к системе или сети. Мы рассмотрим эту тему более подробно в главе 6 «Охота на пользовательские реквизиты».

Приложения

Приложения являются точкой входа для пользователя, который использует данные и передает, обрабатывает или хранит информацию в системе. Приложения стремительно развиваются, и внедрение приложений на основе модели SaaS находится на подъеме. Тем не менее у этого объединения приложений есть унаследованные проблемы. Вот два ключевых примера:

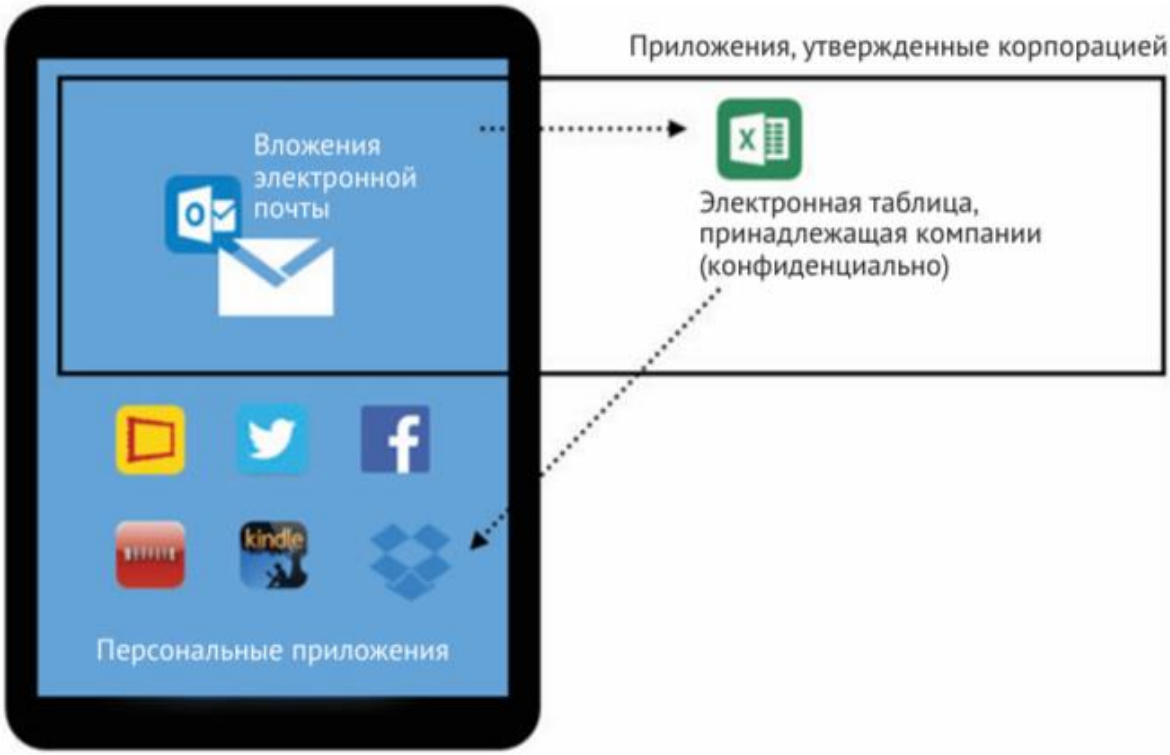
-безопасность (насколько безопасны приложения, которые разрабатываются внутри компании, и приложения, за которые вы платите как за сервис);

-приложения, принадлежащие компании, и персональные приложения (у пользователей будет собственный набор приложений на своих устройствах – сценарий BYOD). Как эти приложения угрожают безопасности компании, и могут ли они привести к потенциальной утечке данных?).

Если у вас есть команда разработчиков, которые создают собственные приложения, следует принять меры, гарантирующие, что они используют безопасную среду на протяжении всего жизненного цикла разработки программного обеспечения, например Microsoft Security Security Lifecycle (SDL). При использовании SaaS-приложения, такого как Office 365, необходимо убедиться, что вы ознакомились с политикой безопасности и соответствия поставщика. В данном случае цель состоит в том, чтобы увидеть, могут ли поставщик и SaaS-приложение соответствовать требованиям безопасности и соответствия вашей компании.

Еще одна проблема безопасности, с которой сталкиваются приложения, заключается в том, как данные компании обрабатываются в разных приложениях, т. е. в тех, которые используются и одобрены компанией, и в тех, которые используются конечным пользователем (личные приложения). Эта проблема становится еще более острой в случае с SaaS, когда пользователи используют множество приложений, которые могут быть небезопасными. Традиционный подход к сетевой безопасности для поддержки приложений не предназначен для защиты данных в SaaS-приложениях. Дело обстоит еще хуже. Они не дают IT-специалистам наглядного представления о том, как их используют сотрудники. Этот сценарий также носит название Shadow IT, и, согласно опросу, проведенному Cloud Security Alliance (CSA) (12), только 8 % компаний знают о масштабах Shadow IT в своих организациях. Вы не можете защитить то, чего не знаете, а это уязвимый момент.

Согласно отчету о глобальных рисках в сфере IT лаборатории Касперского за 2016 г. (13), 54 % предприятий считают, что основные угрозы информационной безопасности связаны с ненадлежащим обменом данными через мобильные устройства. IT-отделам необходимо получать контроль над приложения ми и применять политику безопасности на всех устройствах, принадлежащих компании и BYOD. Один из ключевых сценариев, который вам нужно нейтрализовать, описан на рис.1.2



В этом сценарии у нас имеется личный планшет пользователя, на котором есть утвержденные, а также персональные приложения. Без платформы, которая могла бы интегрировать управление устройствами с управлением приложениями, эта компания подвержена потенциальной утечке данных. В этом случае, если пользователь скачивает электронную таблицу Excel на свое устройство и загружает ее в персональное облачное хранилище Dropbox, а электронная таблица содержит конфиденциальную информацию компании, он создает утечку данных без ведома или возможности компании обезопасить себя.

Данные

Состояние	Описание	Угрозы	Контрмеры	Нарушение трех ключевых принципов информационной безопасности
Данные в состоянии покоя на устройстве пользователя	В настоящее время данные находятся на устройстве пользователя	Несанкционированный или вредоносный процесс может прочитать либо изменить данные	Шифрование данных в состоянии покоя. Это может быть шифрование на уровне файлов или шифрование диска	Конфиденциальность и целостность
Данные в пути	В настоящее время данные передаются с одного хоста на другой	В ходе атаки посредника данные могут быть прочитаны, изменены или похищены	Для шифрования данных при передаче могут быть использованы протоколы SSL/TLS	Конфиденциальность и целостность
Данные в состоянии покоя локально (сервер) или в облаке	Данные находятся в состоянии покоя либо на жестком диске сервера, расположенном локально, либо в облаке (пул хранения)	Несанкционированные или вредоносные процессы могут прочитать или изменить данные	Шифрование данных в состоянии покоя. Это может быть шифрование на уровне файлов или шифрование диска	Конфиденциальность и целостность

Поскольку мы закончили предыдущий раздел, говоря о данных, следует убедиться, что данные всегда защищены, причем независимо от их текущего состояния (в пути или в состоянии покоя). В зависимости от состояния данных угрозы будут разными. Ниже приведены примеры потенциальных угроз и контр меры.

Это всего лишь несколько примеров потенциальных угроз и предлагаемых контрмер. Для полного понимания пути передачи данных в соответствии с потребностями клиента необходимо провести более глубокий анализ. У каждого клиента будут свои особенности, касающиеся пути передачи данных, соответствия, правил и положения. Крайне важно понять эти требования еще до начала проекта.