УДК 004.732

МЕТОДЫ ВНЕДРЕНИЯ МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ В СЕТЕВУЮ ИНФРАСТРУКТУРУ ОРГАНИЗАЦИИ

Яицкий А.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Университет ИТМО»)
Научный руководитель – к.т.н., доцент ФБИТ Гирик А.В.
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Университет ИТМО»)

В докладе представлено описание методов внедрения модели нулевого доверия в сетевую инфраструктуру предприятия, основываясь на стандарте NIST 800-207. Обозначены основные аспекты данной модели и то, какими способами предприятие может модернизировать свою сеть, не прибегая к покупке готового решения.

Введение. Согласно статистике, самой распространенной моделью организации защиты информационной инфраструктуры организаций является защита сети на основе модели сетевого периметра. Однако, такая модель имеет определенные недостатки, связанные, например, с “боковым передвижением” и получением повышенных привилегий и возможностей не уполномоченными сотрудниками или злоумышленниками. Повысить уровень безопасности в сети можно внедрив в инфраструктуру модель нулевого доверия. Это позволит больше контролировать каждое подключение к какому-либо внутреннему ресурсу, а подключения изнутри периметра не будут считаться изначально более надежными, чем снаружи. Ко всем соединениям будут применяться одинаковые методы оценки доверия. Крупнейшими поставщиками услуг внедрения модели нулевого доверия являются Microsoft, Google, Cisco, Palo Alto Networks и другие. Эти решения требуют больших финансовых затрат, поэтому целью данного исследования является разработка и обобщение методов, которые позволят организациям самостоятельно оценить возможность внедрения и самостоятельно модернизировать свою инфраструктуру на основе модели нулевого доверия.

Основная часть. Чтобы привести сетевую инфраструктуру к модели нулевого доверия, требуется постепенное построение и внедрение новых механизмов, структур доступа и политик. Этот процесс подразумевает поэтапную настройку отдельных сегментов с постоянным мониторингом и проверкой функциональности. Соответственно, какой-то период времени, инфраструктура будет представлять собой гибрид модели сетевого периметра и модели нулевого доверия. Допустимо даже оставить без изменений какие-либо аспекты старой сетевой инфраструктуры, если они успешно интегрируются с новыми, а также уровень их защищенности будет устраивать организацию. Касательно методов внедрения модели нулевого доверия, основным ориентиром для соответствия требованиям будет являться стандарт NIST 800-207 “Zero Trust Architecture”.

Для того, чтобы успешно внедрить модель нулевого доверия, первым и обязательным пунктом будет являться инвентаризация активов организации, а также визуализация инфраструктуры. В данном случае не требуется сразу же полностью описывать максимально подробно всю инфраструктуру, допустимо начать с какого-то отдельного актива или сервиса, чтобы протестировать применение принципов и продумать дальнейшие нововведения. Однако, чем подробнее будет описание, тем проще будет анализировать возможные уязвимости и взаимодействия. Для этого нужно будет воспользоваться различными программными средствами мониторинга, анализа трафика и сетевыми агентами. Нужно построить модель, которая будет отображать различные сущности, такие как пользователь, устройства, конечные точки, приложения, сервисы. Это делается для того, чтобы потом была возможность их классифицировать, найти векторы атак, оценить риски.

Далее, когда составлена модель инфраструктуры, нужно обозначить зоны для внедрения нулевого доверия и для сегментации, так как она является основой данной модели,

согласно стандартам. Требуется максимально продумать, как нужно организовать всё так, чтобы соблюдать принцип минимальных привилегий и обеспечить стабильную функциональность. Здесь все зависит от предприятия, так как существует множество вариантов инфраструктур. Но чтобы успешно выполнить микросегментацию, судя по практике внедрения в мире, не хватит обычной настройки межсетевого экрана. Требуется использование программной микросегментации для, например, приложений и сервисов в виртуальных средах или облачных платформ, так как они являются динамичными. Это означает, что зоны и связи описываются с точки зрения логических атрибутов, абстрагированных от базового оборудования и сетей. Политики взаимодействия должны быть основаны именно так, чтобы обеспечить возможность более легкого перемещения и миграции, если она может потребоваться в перспективе. Этот процесс сложен для неподготовленной инфраструктуры, но возможен при использовании современных облачных платформ.

После того, как были обозначены сегменты для модели нулевого доверия, нужно создать политики. За основу берется принцип минимальных привилегий и начальными условиями является недоверие ко всем соединениям. Чтобы обеспечить безопасное подключение субъекта, должна быть использована мультифакторная аутентификация на основе Счетчика доверия, реализованного с помощью программы-агента. Оцениваться уровень доверия будет на точке применения политики, чтобы контролировать подключения через неявную зону доверия, согласно NIST. Для модели нулевого доверия основой является разделение плоскости управления и плоскости данных. Решение о предоставлении доступа осуществляется именно в плоскости управления. Должно быть три различных точки применения политик: на уровне пользователя, сети и приложения. Они интегрируются различными способами с помощью технических систем и бизнес-процессов. Далее они формируют Счетчик доверия и по его результатам предоставляется доступ или отклоняется. Соответственно, пользователю не нужно каждый раз вводить свой пароль, одноразовый пароль, подключаться из одного и того же места, подключаться к одним и тем же приложениям. Настройка политик таким образом упрощает использование и повышает безопасность.

Затем следует применить составленные политики, протестировать интеграцию, наблюдать, как происходит взаимодействие между установленными сегментами и зонами, проанализировать трафик, провести тест на проникновение, сравнить работоспособность. После внедрения модели нулевого доверия в какую-то часть инфраструктуры, можно переходить к следующей и применять указанные методы к ней, в то же время, осуществляя наблюдение и усовершенствование внедренной модели.

Выводы. Модель нулевого доверия для информационной инфраструктуры предприятий распространена во многих сферах, таких как государственный оборонный комплекс (США), медицинские учреждения (Великобритания), а также различные коммерческие организации и корпорации. Она применяется в комбинации с существующими техническими решениями и методами защиты. Чтобы успешно внедрить эту модель, можно воспользоваться приведенными методами и перестроить сетевую инфраструктуру, опираясь на существующие в организации ресурсы, модернизировать её максимально экономно, оценив целесообразность и подведя под стандарты NIST.

Яицкий А.А. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись